

EXHIBIT

20

**EXHIBITS TO PLAINTIFF'S EX PARTE MOTION FOR TEMPORARY
RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

VOLUME IV of V

EXHIBIT 20	Declaration of Sheryl Drexler Attachments A-W	1-364
------------	--	-------

DECLARATION OF SHERYL DREXLER

TABLE OF CONTENTS

I. INTRODUCTION	1
II. USE OF INVESTIGATIVE TECHNIQUES AND RESOURCES	2
A. ELECTRONIC RESOURCES	2
B. OTHER INVESTIGATIVE RESOURCES	4
i. CIVIL INVESTIGATIVE DEMANDS	4
ii. CANADIAN LAWSUIT	6
iii. DOMAIN NAME "WHOIS" INFORMATION	6
iv. CONSUMER COMPLAINTS SUBMITTED TO THE FTC AND ITS LAW ENFORCEMENT PARTNERS	7
v. CONSUMER COMPLAINTS POSTED ONLINE	8
vi. WRITE-UPS ON SOFTWARE SECURITY PROGRAMS	8
III. IDENTIFYING THE SCHEME AND THE INDIVIDUALS AND COMPANIES RESPONSIBLE FOR THE SCHEME	11
A. DANIEL SUNDIN AND INNOVATIVE MARKETING, INC.	11
i. DANIEL SUNDIN'S AND VANTAGE SOFTWARE, INC.'S CONNECTIONS TO IMI SOFTWARE SECURITY PRODUCTS	13
ii. DANIEL SUNDIN AND WINSOFTWARE, LTD	16
iii. SUNDIN'S PAYMENTS FOR DEFENDANT'S SOFTWARE SECURITY PRODUCT ADVERTISEMENTS	18
B. INNOVATIVE MARKETING, INC. AND INNOVATIVE MARKETING UKRAINE	18
i. ROYAL OAK FINANCIAL D/B/A COLLECTION RECOVERY BUREAU ("CRB")	20
C. JAMES RENO	23
i. RENO'S TELEPHONE NUMBERS ASSOCIATED WITH DEFENDANTS' SOFTWARE SECURITY PRODUCTS	25
ii. JAMES RENO'S CONNECTION TO THE DEFENDANTS' SOFTWARE SECURITY PRODUCTS VIA LIMELIGHT NETWORKS	27
iii. RENO'S CONNECTIONS TO OTHER DEFENDANTS	29
iv. SETUPAHOST.NET	30
D. BYTEHOSTING INTERNET SERVICES, LLC	31
E. SAM JAIN	34

F. KRISTY ROSS	36
G. MARC G. D'SOUZA	40
H. MAURICE D'SOUZA	42
I. ATTEMPTS TO HIDE IDENTITY	45
i. FAILURE TO MAINTAIN CORPORATE FORMALITIES	46
ii. USE OF FALSE, INCOMPLETE, OR INCORRECT INFORMATION	47
iii. INTERNATIONAL PRESENCE	49
IV. EVIDENCE OF THE DEFENDANT'S DECEPTIVE PRACTICES	52
A. ADVERTISEMENTS, "SCANNERS," AND FAKE ADVERTISING COMPANIES	52
i. ADVANCEDCLEANER "SCANNERS" AND ADVERTISEMENTS	53
a. REVIEW OF ADVANCEDCLEANER ADVERTISEMENTS	54
b. MISREPRESENTATIONS IN ADVANCEDCLEANER ADVERTISEMENTS	56
ii. WINANTIVIRUS "SCANNERS" AND ADVERTISEMENTS	57
a. REVIEW OF WINANTIVIRUS ADVERTISEMENTS	59
b. MISREPRESENTATIONS IN WINANTIVIRUS ADVERTISEMENTS	61
iii. DRIVECLEANER "SCANNERS" AND ADVERTISEMENTS	62
a. REVIEW OF WINANTIVIRUS ADVERTISEMENTS	63
b. MISPRESENTATIONS IN DRIVECLEANER ADVERTISEMENTS	67
iv. OTHER ADVERTISEMENTS AND "SCANNERS"	69
B. PURCHASES OF ADVANCEDCLEANER AT ADVANCEDCLEANER.COM	70
C. CALLS TO ADVANCEDCLEANER TOLL FREE SUPPORT LINE	73

DECLARATION OF SHERYL DREXLER

PURSUANT TO 28 U.S.C. § 1746

I, Sheryl Drexler, hereby make the following declaration. Unless otherwise indicated, I have personal knowledge of the facts set forth below. If called as a witness, I could and would testify as follows:

I. INTRODUCTION

1. I am an investigator with the Federal Trade Commission's ("FTC" or "Commission") Division of Marketing Practices in Washington, DC. I have served as the investigator on a number of FTC investigations concerning unfair or deceptive practices, including investigations of entities engaged in commerce on the Internet.
2. In March 2007, I was assigned to work on the Commission's investigation of a scheme in which bogus "system scans" were appearing on consumers' computer screens informing them that their computers were infected with viruses, spyware, pornography, illegal files, and/or other malicious files and software. Consumers were instructed to download and purchase particular software security products to cure the purported problems. My investigation focused on the following: (1) identifying those responsible for the scheme; and (2) capturing and analyzing the "system scans" to confirm that the scans were bogus.
3. As explained below, the following companies and individuals are responsible for the scheme: Daniel Sundin (see Section III.A); James Reno (see Sections III.C-III.D); Sam Jain (see Section III.E); Kristy Ross (see Section III.F); Marc D'Souza (see Section III.G); Maurice D'Souza (see Section III.H); Innovative Marketing, Inc. ("IMI" or "Innovative Marketing") (see Sections III.A-III.B); and ByteHosting Internet Services, LLC ("ByteHosting") (see Sections III.C- III.D).

I found that these individuals and companies were associated with the following products and web sites, among others: *amaena.com*, *advancedcleaner.com* (AdvancedCleaner), *billingnow.com*, *drivecleaner.com* (DriveCleaner), *errorprotector.com* (ErrorProtector), *errorsafe.com* (ErrorSafe), *innovativemarketing.com*, *forceup.com*, *popupguard.com* (PopUpGuard), *setupahost.net*, *supportsw.com*, *vantagesoftware.com*, *virussw.com*, *winantispyware.com* (WinAntiSpyware), and *winantivirus.com* (WinAntiVirus). I also reviewed a number of Defendants' advertisements that purport to "scan" consumers' computers to detect privacy or security issues and determined that no actual scans occurred. See Section IV.A.

4. Section II of this declaration describes the investigative techniques and resources I used to document the deception and determine the responsible parties. Section III reveals each of the Defendants' roles in the scheme. Finally, Section IV describes the evidence I collected concerning the Defendants' web sites, advertisements, and fake "scanners."

II. USE OF INVESTIGATIVE TECHNIQUES AND RESOURCES

A. ELECTRONIC RESOURCES

5. Throughout the course of this investigation, in order to conduct research on the Defendants' web sites and advertisements, view the web sites and advertisements, download the software offered by the Defendants and analyze the resulting effects on the computer, I used two types of computers located in the FTC Internet Lab: (1) standard FTC Internet Lab computers (or machines) and (2) a VMWare computer (or machine). The standard computers have various evidence capture software tools installed on them. These computers are separate from the FTC network and they run Windows XP Professional with the latest software and security patches.
6. The second type of computer, a VMWare computer ("VMWare machine"), creates and allows

one or more virtual machines to run simultaneously within the operating system (“VMWare image”). For the purposes of this investigation, I used a VMWare machine in the FTC Internet Lab to access my password protected VMWare images. After infecting a VMWare image with malicious programs, the computer can be restored to an uninfected state by discarding the infected image and restarting the image again. The VMWare images I used were running Windows XP Professional with no software and security updates, unless otherwise indicated. In all but one case (see Paragraph 196), these VMWare images were created by Todd McLaughlin. See Declarations of Todd McLaughlin and Tina M. Del Beccaro explaining how the FTC ensures that VMWare images do not contain adult content or malicious files.

7. One of the programs installed on both types of FTC Internet Lab computers and utilized throughout the investigation is called Wireshark. Wireshark is a “network protocol analyzer” that captures the Internet Protocol address (“IP address”) and other related information for each Internet data packet traveling to and from the computer. Wireshark decodes and outputs the packets’ data into a log which allows the user to analyze IP address and other information contained within each Internet packet.
8. Throughout the investigation I also utilized an evidence capture computer program called “Camtasia” that is installed on both types of computers in the FTC Internet Lab. Camtasia records a video of any action that appears on the computer screen and saves the recording electronically. In order to create some of the attached images for this declaration from the Camtasia recorder, I used Windows Media Player or the “Camtasia Player” to play back the Camtasia recordings I created. I paused Windows Media Player or the Camtasia Player as I played back a Camtasia recording and pressed the “Print Screen” button on my keyboard to

capture the paused image. I then pasted this image into Microsoft PowerPoint and sized it to fit on the page.

9. Additionally, a program called Snag-It was used to capture images and web sites. Snag-It is installed on both types of computers in the FTC Internet Lab and allows users to capture a picture of the computer screen or a web site and save the image electronically.

B. OTHER INVESTIGATIVE RESOURCES
i. CIVIL INVESTIGATIVE DEMANDS

10. Throughout the course of the investigation, the Commission sent Civil Investigative Demands (“CIDs”) to several different entities. A summary of each of the CIDs discussed in this declaration follows.
11. The Commission sent a CID to TUCOWS, Inc. (“TUCOWS CID response”), the registrar of record for many of the domain names associated with the Defendants, to find out additional information on the registrant(s). The TUCOWS CID also included a list of other domains registered to the same individuals or companies.
12. The Commission sent a CID to Microsoft Corporation (“Microsoft”) for documents obtained as part of the investigation and lawsuit, *Microsoft Corporation v. John Does 1-20, d/b/a/ Amaena.com* (“Microsoft CID response”). The Microsoft CID response included: documents from Royal Oak Financial d/b/a Collection Recovery Bureau (“CRB”) a collection agency, that was hired to collect payment from consumers who disputed charges for Defendants’ software products; and MyGeek.com, Inc. (“MyGeek”) an online advertising company.
13. The Commission sent a CID to both Visa USA, Inc. (“Visa CID response”) and Mastercard International (“Mastercard CID response”) to obtain information on several merchant identifiers

including, “Winsoftware,” “WINS,” and any merchant identifiers with the phone number (800) 755-5909, that were used to process payments for Defendants’ software security products.

14. The Commission sent a CID to Bank of America (“Bank of America CID response”) for account information related to a credit card listed in the MyGeek documents included in the Microsoft CID response.
15. The Commission sent a CID to Junction Networks (“Junction Networks CID response”), the telephone provider for the phone number (800) 755-5909, which is associated with many of the Defendants’ software security products and credit card merchant identifiers.
16. The Commission sent a CID to Limelight Networks, Inc. (“Limelight CID response”) to determine the subscriber associated with the IP address, 208.111.153.244, which I determined was the download location for one of the Defendants’ software security products. Limelight Networks, Inc. (“Limelight Networks”) enables high bandwidth users to distribute their content across the Internet. See Paragraph 77 for more information on Limelight Networks.
17. The Commission sent a CID to US Bank (“US Bank CID response”) for information on ByteHosting Internet Services, LLC’s bank account.
18. The Commission sent a CID to Verizon Wireless (“Verizon CID response”) for information on James Reno’s cellular telephone records.
19. The Commission sent a CID to Sprint Nextel Communications (“Sprint CID response”) to obtain Kristy Ross’s cellular telephone records.
20. The Commission sent a CID to Yahoo! Inc. (“Yahoo! CID response”) to obtain information on email accounts listed in Whois registration records for domains names used by the Defendants.

ii. CANADIAN LAWSUIT

21. During the course of the investigation, the Commission learned about a lawsuit filed in the Ontario Superior Court of Canada. The lawsuit, *Innovative Marketing, Inc. v. Marc Gerard D'Souza et al.*, ("Canadian lawsuit") was originally filed in or about February 2007. See Declaration of Carmen Christopher, Exhibit 17. The Claim (see Ex. 17, Attach. A) alleges that Marc and Maurice D'Souza embezzled \$48 million from IMI. The Statement of Defence and Counterclaim of the Defendant Marc Gerard D'Souza ("Counterclaim") (see Ex. 17, Attach. B) states, "Marc hereby makes claim against Jain and Sundin for: . . . Damages for breach of fiduciary duty to the Business partnership." See Ex. 17, Attach. B, ¶ 225. Also reviewed during the course of the investigation, were several sworn affidavits (see Ex. 17, Attachs. D, F-M) and a Further Fresh as Amended Statement of Defence and Counterclaim of the Defendant Marc Gerard D'Souza ("Further Fresh Counterclaim") (see Ex. 17, Attach. D) that were part of the Canadian lawsuit.

iii. DOMAIN NAME "WHOIS" INFORMATION

22. During the course of the investigation, I reviewed numerous web sites. In order to determine the registrant of these domain names, I retrieved information from a publicly-available database known as a "Whois" database. The Whois information is important because this is where the general public and law enforcement go to obtain contact information about a web site, especially if there is no active web site or if contact information cannot be found on the web site. I used a Whois database located at <http://www.domaintools.com> ("*domaintools.com*"). Unless otherwise noted, references in this declaration to the registrant and the IP address information shown in the Domain Tools records refer to the registrant and IP information as of the date of the search.

23. *Domaintools.com* permits paying members to view “Whois history” records which show a Whois record as it was captured on a previous date. Many of the Defendants’ domains appear in the Whois History section of *domaintools.com*, some going back to 2004 or earlier. I reviewed the Whois History records for many of the Defendants’ domain names.
24. A number of the Whois results I viewed listed incomplete Whois information and/or foreign registrant information. Included as **Attachment A** is a summary of the domain name registration information for some of Defendants’ domain names obtained from *domaintools.com* and from the TUCOWS CID response. See Paragraph 38. The column marked “Source” indicates whether the registrant information was obtained through a Whois record I obtained, a Whois history record or from TUCOWS, Inc. Included as **Attachment B** is true and correct copy of the TUCOWS CID response.

iv. CONSUMER COMPLAINTS SUBMITTED TO THE FTC AND ITS LAW ENFORCEMENT PARTNERS

25. During the course of the investigation, I reviewed many complaints about Defendants’ security products from the FTC’s consumer complaint database, Consumer Sentinel. Consumer Sentinel is the Commission’s central consumer protection complaint databases. It includes consumer complaints mailed to the Commission, entered on the Commission’s web site (www.ftc.gov), and telephoned to the Commission (877-FTC-Help). The Consumer Sentinel database also includes complaints forwarded by or entered directly into the database by a number of other law enforcement authorities and consumer protection organizations around the world.
26. There were over a 1,000 non-duplicative complaints from consumers throughout the United States and around the world regarding the Defendants, their companies, and their products. In

addition to complaints about fake scanners, the consumers complained about: software being downloaded onto their computers without their permission, reduced performance of their computer, loss of work, incessant pop-ups, the inability to connect to the Internet, the computer becoming inoperable, and the inability to remove the software. Consumers also complained that they were charged for additional services that they did not agree to when purchasing the products, were promised a refund by the Defendants' customer support representatives, which was not honored, the inability to easily contact the company, and that they could not find the name of the company or the individuals behind the software or billing companies. Many of the consumer complaints I analyzed were from consumers who thought that the pop-up advertisements for software security products received from the Defendants were associated with either their antivirus/antispyware program and/or from the Windows operating system.

v. CONSUMER COMPLAINTS POSTED ONLINE

27. During the course of the investigation, I performed Google searches on the Defendants, their companies and their software security products. Each query produced thousands of results. During the course of the investigation, I reviewed numerous links from these queries. Many of the hits in the results were for online forums that discuss spyware or other technical issues and included consumers complaining about the software security products, the inability to find who is responsible, and/or seeking help on how to stop the advertisements and/or remove the programs.

vi. WRITE-UPS ON SOFTWARE SECURITY PROGRAMS

28. During the course of the investigation, I also researched the Defendants' software security products and their associated web sites. I obtained these write-ups from several companies that

manufacture anti-spyware products including but not limited to: Computer Associates, F-Secure, Kaspersky, McAfee, Inc., Microsoft Corp., Panda Software, ParetoLogic, PCTools, Sophos Plc., Sunbelt Software, Inc., Symantec Corp., and Tenebril, Inc. Included as **Attachment C** are true and correct copies of write-ups from several of these companies including but not limited to some of the following products: AdvancedCleaner, DriveCleaner, Errorsafe, WinAntiSpyware, WinAntiVirus, and WinFixer.

29. In Microsoft's "Security Intelligence Report July through December 2007" available at <http://www.microsoft.com/downloads/details.aspx?familyid=671355c2-4002-4671-8619-95c96c8a897f&displaylang=en&tm>, the top "Rogue Security Software Families" are discussed. Microsoft states, "Rogue security software uses a number of different techniques to attempt to trick users into installing the software and to obtain money from them." The number one "Rogue Security Software Family" observed during this period was Winfixer with 3,382,135 infections detected in the second half of 2007. Also included in the top 25 rogue security software families were WinSoftware (#4), DriveCleaner (#8), AdvancedCleaner (#9), and SystemDoctor (#17). All of these families are connected to the Defendants. Included as **Attachment D** is a true and correct copy of the chart of "Rogue Security Software Families" included in the Microsoft report.
30. I also obtained write-ups from McAfee SiteAdvisor on or about October 27, 2008. McAfee, Inc., a company that manufactures anti-spyware and anti-virus products, runs the web site located at <http://www.siteadvisor.com> ("SiteAdvisor"). According to the web site, SiteAdvisor is a site designed to warn consumers about online scams and web sites that may result in spyware, spam, and viruses. SiteAdvisor categorizes web pages into red (unsafe), yellow (questionable)

and green (safe) ratings based on “automated safety tests of web sites.” I entered the following domains associated with the Defendants: *advancedcleaner.com*, *drivecleaner.com*, *errorprotector*, *winadblocker.com*, *winantispy.com*, *winantispyware.com*, *winantivirus.com*, *wincontentfilter.com*, *windrivecleaner.com*, *winfixer.com*, and *winsoftware.com* into McAfee SiteAdvisor’s analysis page. Each of these domains were rated as “red” due to content found on the sites that may be considered “adware, spyware or other unwanted programs.” Several of these reports also included comments and complaints from SiteAdvisor users who included warnings about these web sites. Included as **Attachment E** are true and correct copies of the reports I obtained from McAfee SiteAdvisor on these web sites.

31. On or about October 27, 2008, I visited the web site located at <http://www.stopbadware.org> (“Stopbadware”), a joint project of Harvard Law School’s Berkman Center for Internet & Society and Oxford University’s Oxford Internet Institute. According to Stopbadware, the web site was created to provide reliable objective information about downloadable applications in order to help consumers make better choices about what they download on to their computers. Stopbadware tests and reports on applications and posts their findings in a report on their web site. I viewed and printed the reports from Stopbadware regarding: Drive Cleaner 2006 (Free Version), PerformanceOptimizer, WinAntiSpyware 2006 (Unregistered Version), WinAntiVirus 2006, and XP Antivirus 2008. All of these reports warn against downloading these programs and concluded that, among other behaviors the software or programs “install deceptively,” “does not clearly identify itself,” “interferes with the user’s normal computer usage,” “displays pop-up ads,” “makes exaggerated claims of system vulnerability,” “downloads updates without user’s consent,” “automatically runs on startup,” “continuously runs a process in the background,” and

“is not easy to uninstall completely.” Additionally, Stopbadware found the programs are sold using “fear tactics” including false pop-up ads or alerts that look “almost identical to a Windows’ generated warning.” These pop-up ads or alerts purport to detect a large number of non-existent “dangerous,” “critical,” or “compromising” files. These findings are consistent with my experiences and/or those listed in the consumer complaints I reviewed. See Sections IV and Section I.B(iv) above. Included as **Attachment F** are true and correct copies of the Stopbadware reports I printed.

32. Throughout the course of the investigation, I also observed several of Defendants’ web sites for software security products being listed as potentially dangerous by Google. For example, on or about October 27, 2008, when I entered the term, “drivecleaner.com” into Google’s search bar and executed the query, the first result said, “DriveCleaner - Home” and beneath this text it read, “This site may harm your computer.” When I entered this site into Google’s “Safe Browsing Diagnostic page” located at <http://www.google.com/safebrowsing/diagnostic?site=x> (where “x” is equal to the web site the user would like to review), I found the diagnostic pages for both <http://www.drivecleaner.com> and <http://www.systemdoctor.com> read, “Site is listed as suspicious- visiting this web site may harm your computer.” Included as **Attachment G** is a sample of the Google result for *drivecleaner.com*.

III. IDENTIFYING THE SCHEME AND THE INDIVIDUALS AND COMPANIES RESPONSIBLE FOR THE SCHEME

A. DANIEL SUNDIN AND INNOVATIVE MARKETING, INC.

33. As established in this section, Daniel Sundin is the Chief Technology Officer of Innovative Marketing, Inc. as well as the chief designer of Innovative Marketing’s software products. He

formerly acted as the Chief Operating Officer of IMI. He is the CEO/Director of Winsoftware. He registered domains names, including *innovativemarketing.com*, using the company name Vantage Software, Inc. Daniel Sundin paid for advertisements for Defendants' software security products with companies such as MyGeek.

34. In Daniel Sundin's Affidavit in the Canadian lawsuit sworn February 19, 2007, he acknowledges he serves as Chief Technology Officer of IMI beginning in December 2005 and he lives in London in the United Kingdom. See Ex. 17, Attach. G, ¶ 1. Prior to this function, he acted in the role of Chief Operating Officer of IMI. See Ex. 17, Attach. G, ¶ 1. He incorporated Innovative Marketing, Inc. on or about July 18, 2002 as a Belize corporation. He lists the following software security product web sites as associated with IMI: *winantivirus.com*, *winadblocker.com*, *winantispy.com*, *wincontentfilter.com*, *windrivecleaner.com*, *drivecleaner.com*, *multimediafixer.com*, *computershield.com*, *pcsupercharger.com*, *stopguard.com*, and *popupguard.com*. See Ex. 17, Attach. G, ¶ 9.
35. Throughout the course of the investigation I used the Law Enforcement Solutions databases of LexisNexis, located at <http://www.lexis.com>, to find information on Daniel Sundin. Between 2000 and 2004 there were various addresses listed in Washington state and Arizona for Daniel Sundin.
36. According to the Claim in the Canadian lawsuit, while serving as both Chief Operating Officer and Chief Technology Officer of IMI, Daniel Sundin also acted as the chief designer of IMI's software security products. See Ex. 17, Attach. A, ¶ 22.
37. Sundin's Affidavit in the Canadian lawsuit sworn February 19, 2007, also states that Innovative

Marketing has offices in Kiev, Ukraine, in Bangalore, India, and in Buenos Aires, Argentina. The Kiev, Ukraine office began operations in approximately December 2001 and serves as the corporate headquarters. Sundin states that the facility in Kiev employs approximately 300 people, the Argentina office employs about 45 people and the office in India employs approximately 35 people. Among other responsibilities, these employees “localize the products into every international language.” See Ex. 17, Attach. G, ¶ 10-11.

i. DANIEL SUNDIN’S AND VANTAGE SOFTWARE, INC.’S CONNECTIONS TO IMI SOFTWARE SECURITY PRODUCTS

38. Several of the domain names included as part of the TUCOWS CID response identified the registrant and/or reseller and/or company name as “Vantage Software, Inc.” (“Vantage” or “Vantage Software.”) The technical contact listed for the domain, *vantagesoftware.com* also includes the email address *daniel.sundin@engelholm.se*.
39. Several of these domains included in the TUCOWS CID response list Innovative Marketing, Inc. at 1876 Hutson Street in Belize as the reseller’s technical contact, along with the email address *hostmaster@innovativemarketing.com*. Prior domain registration information for *winfixer.com* includes an address in the Ukraine instead of Belize. See Attachment A.
40. Pleadings from the Canadian lawsuit, *Innovative Marketing, Inc. v. Marc Gerard D’Souza et al.* verify this information. Included as an exhibit to the Affidavit of Daniel Sundin sworn March 6, 2007 is a “Registration Service Provider Agreement” (“RSP Agreement”) between TUCOWS, Inc. and Vantage Software, Inc. authorizing Sundin to resell domain names. The agreement is signed by Daniel Sundin, President of Vantage Software and in the agreement, he provides the

referenced the software products called "PopupGuard" and "DriveCleaner." The domain *drivecleaner.com* shares an IP address with *popupguard.com* and is registered to Innovative Marketing, Inc. at 1876 Hutson Street in Belize, the same address listed for the *vantagesoftware.com* reseller account with TUCOWS, Inc. Daniel Sundin also registered the domain *innovativemarketing.com* with TUCOWS, Inc.

44. I also viewed the billing page for *popupguard.com* on or about May 1, 2008. When I clicked on the link to download PopupGuard, I was redirected to <https://secure.billingnow.com> . . . I then viewed the web page's certificate by selecting the menu marked, "Page" in Internet Explorer 7 ("IE 7") and selecting "Security Report." I then clicked on the option, "View certificates" and selected the tab labeled "Details." I then clicked on "Subject" and it read "Website Security, Billingnow.com, 22 Carnegie Crescent, Thornhill, ONT, CA L3T 5H1." It also read, "Hosted by Setup A Host, Inc." The domain *setupahost.net* resides on the same IP address as both *drivecleaner.com* and *popupguard.com*. Several other web sites listed, "Hosted by Setup A Host, Inc." in the subject information of the sites' security certificates including: *drivecleaner.com*, *errorprotector.com*, and *winantispyware.com*. See Paragraph 90 below for additional information on these security certificates.

45. Both *innovativemarketing.com* and the domain *drivecleaner.net* were once registered to Vantage Software, Inc. at 2711 Centerville Road in Wilmington, DE. The registration information for the domain *drivecleaner.net* also lists the email address *daniel.sundin@engelholm.se*. See **Attachment A.**

46. Daniel Sundin's Affidavit dated February 19, 2007, from the Canadian lawsuit, includes an

same email address, *daniel.sundin@engelholm.se*, that is listed in the TUCOWS CID response. See Ex. 17, Attach. I, ¶ 4, 6 and Sundin Exhibit A. Sundin has used the authority granted by the reseller agreement to purchase domain names for the Defendants including *innovativemarketing.com*. See Attachment A.

41. Included as part of the exhibit to Sundin's Affidavit in the Canadian lawsuit sworn March 6, 2007, are several invoices from TUCOWS, Inc. to "Vantage" in which the company being billed for domain names is Innovative Marketing, Inc. at 1876 Hutson Street in Belize. See Ex. 17, Attach. I, ¶ 4, 6 and Sundin Exhibit A.
42. On several occasions throughout the investigation, I performed a reverse Internet Protocol ("IP") search for Defendants' web sites and IP addresses using *domaintools.com*. A reverse IP search lists other domain names hosted at the same IP address. In my experience, when there is a relatively small number of domains hosted on the same IP address, the sites tend to be connected. This can also be confirmed by looking for consistencies in the current and historical Whois information for domains located on the same IP address. Several of Vantage's domains including *winantivirus.com* and *errorprotector.com* share the same IP address. The domain name, *popupguard.com* also shares an IP address with *winantivirus.com* and *errorprotector.com* as well as with the domains, *billingnow.com*, *drivecleaner.com*, *setupahost.net*, and *virussw.com*. A true and correct copy of the reverse IP logs for 66.244.254.46, 66.244.254.63, 83.170.116.39, 85.17.4.103, and 190.15.73.254 are included as **Attachment H**.
43. On or about May 1, 2008, I used a computer in the FTC's Internet Lab to visit the web site, *http://www.popupguard.com* ("*popupguard.com*"). The homepage for *popupguard.com*

exhibit that depicts the steps a consumer would go through in order to purchase DriveCleaner through one of IMI's web sites. The Exhibit consists of screenshots that are nearly identical to the advertisements, web sites, and downloads I observed during the course of the investigation. See Section IV for additional information on the advertisements I reviewed. Each screenshot also includes a description of the consumer's experience and additional information. Underneath the screenshot of the installer, it reads, "Installers are commonly distributed via Limelight servers," which I confirmed via downloads of Defendants' software security products and the Limelight CID response. See Paragraphs 77 and 78 for additional information on Limelight Networks. These screenshots looked identical to the one mentioned in Paragraph 199. See Ex. 17, Att. G, ¶ 13 and Sundin Exhibit D.

47. The domain *popupguard.com* is registered to "Vantage Software Inc., Ltd" at Green Dragon House, 64-70 High Street, Croydon, Surrey CR09XN with the email address *hostmaster@popupguard.com*. A Whois history record from *domaintools.com* from December 20, 2003 shows *popupguard.com* as previously being registered to Vantage Software, Inc. at 2711 Centerville Road, Wilmington, DE 19808 with the email address *daniel.sundin@engelholm.se*. The phone number is listed as 555-123-1234. This is the same fake telephone number that appears in numerous domains registered to IMI.

ii. DANIEL SUNDIN AND WINSOFTWARE, LTD

48. On or about April 29, 2008, I used the Law Enforcement Solutions databases of LexisNexis, located at *http://www.lexis.com*, to find information on Daniel Sundin. According to Dun & Bradstreet ("D&B"), Daniel Sundin is listed as the CEO/Director of Winsoftware, Ltd at Green

Dragon House, 64-70 High Street, Croydon, Surrey CR09XN. This is the same address listed in the Whois record for *popupguard.com*. Winsoftware's description in the D&B Information Report lists "prepackaged software." **Attachment I** is a true and correct copy of this record.

49. Both *vantagesoftware.com* and *winsoftware.com* share the IP address 66.244.254.46 along with *winantispay.com*, *windrivecleaner.com*, and *wincontentfilter.com*. These three sites were all registered to IMI in Belize. See Attachment A and H.
50. Both current and past versions of some of the Defendants' software security product web sites in **Attachment A**, list "Winsoftware" in the "legal" section of the sites. For example, the License Agreement for WinAntiSpyware found at *winantispayware.com* indicates the software is the property of Winsoftware.
51. On or about May 2, 2008, I visited the web site located at <http://www.winsoftware.com> using a computer in the FTC's Internet Lab. On the page labeled, "Store" there are links to purchase "WinPrivacyGuard," "WinAntiVirus 2005 Pro," "WinAntiSpam 2005" and "WinContentFilter." *Wincontentfilter.com* and *winantivirus.com* are both listed by Daniel Sundin as IMI software security product web sites in the Canadian lawsuit. See Paragraph 34. Included as **Attachment J** are true and correct copies of selected pages of *winsoftware.com*.
52. Throughout the page titled, "Refund and Return Policy," the company name is listed as Winsoftware Ltd. When I clicked on the link labeled, "Store," and selected "WinAntiVirus Pro 2006," it read, "Winsolutions, FZ LCC" at the bottom of the page. The License Agreement for WinAntivirusPro 2006 also references Winsoftware Corporation, Inc. and makes reference to 24/7 customer service. See Attachment J.

iii. SUNDIN'S PAYMENTS FOR DEFENDANT'S SOFTWARE SECURITY PRODUCT ADVERTISEMENTS

53. Daniel Sundin paid for advertisements that Defendant Kristy Ross placed with MyGeek, an advertising network. Included in the Microsoft CID response were documents from MyGeek which included a chart of credit card numbers used to pay for advertisements. One of these credit card numbers was listed with Daniel Sundin's name and an address in Seattle, Washington. I determined that the issuing bank of this credit card was Bank of America and the Commission subsequently sent a CID to Bank of America for information on this credit card and account holder. Included in the Bank of America CID response, was a Secured Card Application which showed Daniel Sundin's name in connection with "Vantage Software, Inc." and the email address *daniel.sundin@engleholm.se*, the same email address listed in Whois results as described above. Included as **Attachment K** is a true and correct copy of the Secured Card Application. Personally identifiable information has been redacted.

B. INNOVATIVE MARKETING, INC. AND INNOVATIVE MARKETING UKRAINE

54. As established in this section, Innovative Marketing is the corporate entity the Defendants use to market and sell their software security products. Several of the domain names included as part of the TUCOWS CID response identified the registrant and/or company name as "Innovative Marketing, Inc." Additionally, as indicated in the chart included as **Attachment A**, many of the Defendants' domains used the address at 1876 Hutson Street, Belize City, Belize and the email address *hostmaster@innovativemarketing.com* either in the current Whois record or in the Whois history record. This is the same address and email address that Daniel Sundin provided to TUCOWS Inc. in connection with the Vantage Software reseller account.

55. On or about May 2, 2008, I used a computer in the FTC Internet Lab to visit the web site located at <http://www.innovativemarketing.com>. I clicked on the tab that read, "Products" and the text read,

Our software works to optimize your computer's potential. We have developed software that will protect your computer against worms, viruses, and other diseases that infect it. While others help to 'clean' your computer from unwanted elements that tend to slow down your computer's response time.

It then reads, "the issue of privacy has become a worry of many consumers . . . our products have been developed to protect your computer . . . to assume your identity's safety." Included as **Attachment L** is a true and correct copy of selected pages of *innovativemarketing.com*.

56. On or about August 2, 2007, I used a VMWare computer in the FTC Internet Lab to purchase "WinAntiSpyware" with an undercover credit card. The onscreen confirmation for this purchase indicated my credit card statement would list *virussw.com* and the phone number (800) 755-5909. However, the purchase appeared on the undercover Visa credit card I used as *supportsw.com* instead of *virussw.com*, and listed the phone number (800) 755-5909. This phone number is assigned to Defendant James Reno. See Paragraph 71 below. Included as **Attachment M** is a true and correct copy of the email confirmation of my order of WinAntiSpyware and the undercover credit card statement. Personally identifiable information has been redacted.

57. On or about, March 12, 2008, I used a VMWare computer in the FTC Internet Lab to purchase "AdvancedCleaner." See Section IV.B for further information on this transaction. The purchase appeared on the undercover Visa credit card I used as "supportsw.com 8007555909." The phone

number (800) 889-5113 also appeared on my online confirmation. This phone number is assigned to Defendant James Reno. See Paragraph 71 below. Included as **Attachment N** is a true and correct copy of the email confirmation of my order of AdvancedCleaner, the onscreen confirmation and the undercover credit card statement. Personally identifiable information has been redacted.

58. The Commission sent a CID to Visa USA, Inc. and Mastercard International to obtain information on several merchant identifiers including, "Winsoftware" and the phone number (800) 755-5909. These CIDs also requested the number of orders and the total amount in sales. From 2005 to 2007 there were over one million transactions processed under the merchant identifiers including the names, "Winsoftware," "Supportsw," "Virussw," "WINS," "Securitysw," "Errorsafe," "Winfixer," Driveclnr," "Antivirussw" and/or the phone number, (800) 755-5909. The merchant names listed are consistent with many of the Defendants' web sites and products I reviewed during the course of the investigation, such as *drivecleaner.com* and *errorsafe.com*. During this two year period, these Visa merchant identifiers had a total of over \$53 million in sales.

i. ROYAL OAK FINANCIAL D/B/A COLLECTION RECOVERY BUREAU ("CRB")

59. The Microsoft CID response included documents from Royal Oak Financial d/b/a Collection Recovery Bureau (CRB). Several of the email communications between CRB and the Defendants' companies came from email addresses from *innovativemarketing.com.ua* and *winsoftware.com*. The country code ".UA" stands for Ukraine, and as shown in **Attachment A** several of the domains that advertise Defendants' software products are currently or were

previously registered to addresses in the Ukraine and/or use the name Innovative Marketing as the registrant.

60. An email message from “Alexandr” with the email address, *kurbik@innovativemarketing.com.ua*, included information for a bank account named “Web Integrated Net Solutions” in Bahrain for which payments collected by CRB should be deposited. I believe “Web Integrated Net Solutions” is the full name for the merchant identifier, “WINS,” which appeared in the Mastercard and Visa CID responses mentioned in Paragraph 58.
61. An email message dated November 7, 2006, from *cathy@winsoftware.com* indicates that the telephone number “18007555909” should be listed in conjunction with purchases for DriveCleaner. A later email message, dated January 17, 2007, shows a consumer’s purchase information for WinAntiVirus Pro 2006. The email lists the web site *winantiviruspro.com*, the telephone number 1-800-755-5909, and indicated the charge will appear on the customer’s credit card as “Security SW.” This merchant name also appeared in the Visa and Mastercard CID responses and this is the same telephone number that appeared on my undercover Visa credit card statement after purchasing WinAntiSpyware and AdvancedCleaner.
62. An email from *alexandr@innovativemarketing.com.ua* advises CRB that the “CS” (which I believe to mean Customer Support) is “1-800-755-5909 (USA)” and “our contact e-mail is like support@(depend on product) For instance *www.winantivirus.com* contact e-mail is *support@winantivirus.com*.” After completing the purchase of WinAntiSpyware I received email messages from *support@winsoftware.com* and after purchasing AdvancedCleaner, I was informed by the customer service representative who answered the technical support line that I

could contact support@advancedcleaner.com for additional questions regarding the product.

See Section IV.C for information about my call to the AdvancedCleaner toll free support line.

63. A list of over 1,000 accounts submitted for collection by IMI to CRB was included in an email between IMI representatives and CRB. The table below indicates the product name and the web site listed for that product from which the consumer made the purchase based on the list of collection accounts. Each of these domains appears in the chart included as **Attachment A**.

Product	Associated Web Site
Winfixer 2005 and 2006	winfixer.com
WinAntiSpyware 2005 and 2006	winantispyware.com
WinAntiVirusPro 2006	winantivirus.com
ErrorSafe	errorsafe.com
Sysprotect	sysprotect.com
SystemDoctor	systemdoctor.com
DriveCleaner	drivecleaner.com

A true and correct copy of this email message has been included as **Attachment O**. Due to the size, only the first page of the list of accounts has been included and personally identifiable information for the customers has been redacted.

64. An email chain from kurbik@innovativemarketing.com.ua dated January 27, 2007 indicates that there is new bank account information. At the bottom of the email message there are “payment details for wire” which list Sunwell Incorporation in Belize, with the beneficiary bank in Riga, Latvia. Several of the collection accounts are for products where the associated web sites are currently or previously were registered in Belize and to IMI. See **Attachment A**. Included as

Attachment P is a true and correct copy of this email message. Financial account numbers have been redacted.

C. JAMES RENO

65. As established in this section, James Reno is the President of ByteHosting Internet Services, LLC based in Ohio which was paid by several companies including Sunwell and Winpayment Consultancy SPC, all of which are affiliated with IMI. James Reno is the subscriber of several telephone numbers used in connection with the Defendants software security products and several of these numbers are associated with the merchant identifiers consumers see on their credit card statements when purchasing one of the Defendants' software security products. His mother, Cathy Walton, is the call center manager for Defendants' software security products. James Reno is listed as the contact with Limelight Networks, Inc., the content delivery network used for Defendants' software security products. See Paragraph 77 for additional information on content delivery networks. He uses the email address *james@setupahost.net*, which is associated with the company Setup A Host. Set Up a Host is used in connection with Defendants' software security products. He also uses the email address *mydomains@yahoo.com* which is listed in the registration information for *forceup.com*, one of the defendant's fake advertising companies. See Paragraph 147. James Reno was a party in the Symantec lawsuit (see Paragraph 102) along with Sam Jain and Innovative Marketing, Inc., among others and was also sued in a private lawsuit filed in 2006 involving Defendants' software security products. See Paragraph 69.
66. On or about April 15, 2008, I used the Law Enforcement Solutions databases of LexisNexis to

obtain information on James Reno in Ohio. I found a James Reno and a Catherine Walton (a.k.a. Cathy Reno and Cathy Walton) listed at 2864 Lindale Mount Holly Road, Amelia, OH 45102. According to the information in LexisNexis, James Reno was born in 1983 and Catherine Walton was born in 1960. I believe that Catherine Walton (a.k.a. Cathy Walton) is James Reno's mother.

67. On or about April 23, 2008, I repeated the search I had previously run on James Reno in the LexisNexis Law Enforcement Solutions database. James Reno had a new current address listed as of April 2008. The address was listed as 3844 Golden Meadow Court, Amelia, OH 45102. The Commission obtained a driver's license record for James Reno which lists both of these addresses in Ohio.
68. On or about December 11, 2007, I visited the web site located at <http://www.jamesreno.com>. This site is registered to Byte Hosting Internet Services, LLC. According to the web site, James Reno is knowledgeable in several computer languages, protocols, and technologies, is familiar with various software programs and operating systems, including, Linux, Apache Web Server, MySQL Database Server, PHP, and Unix. He also has experience with computer hardware. Included as **Attachment Q** is a true and correct copy of printouts of [jamesreno.com](http://www.jamesreno.com).
69. On or about September 29, 2006, a lawsuit was filed in the state of California, *Beatrice Ochoa v. Marc J. Cohen and Does 1 through 100*. The Complaint filed in the suit was later amended to include James Reno and ByteHosting Internet Services, LLC. The lawsuit alleged WinFixer, ErrorSafe, WinAntiVirus and WinAntiSpyware were "fraudware products," which "report that the host computer is infected regardless of the truth" and then "misrepresent[] that the victim

may repair the purported problem by paying money” to the Defendants. This lawsuit was dismissed in or about September 2007. Included as **Attachment R** is a true and correct copy of the Complaint and the docket in this lawsuit.

i. RENO’S TELEPHONE NUMBERS ASSOCIATED WITH DEFENDANTS’ SOFTWARE SECURITY PRODUCTS

70. The telephone number (800) 755-5909, as established below, is assigned to James Reno. This telephone number is listed as part of several merchant account names obtained from Visa and Mastercard (see Paragraph 58) and was listed in the confirmation for my undercover purchases of WinAntiSpyware and AdvancedCleaner.
71. According to the Junction Networks CID response, the phone number (800) 755-5909 is assigned to: James Reno, ByteHosting Internet Services, LLC, 3864 McMann Road, Cincinnati, OH 45245. The CID response also included following additional phone numbers assigned to James Reno of ByteHosting Internet Services, LLC, including the telephone numbers (202) 904-2212, (800) 430-8969, (800) 431-3496, (800) 467-1077, (800) 608-3716, (877) 405-5229, (877) 871-7412 and (800) 889-5113 which are also associated with Defendants’ software security products. Included as **Attachment S** is a true and correct copy of relevant pages of the Junction Networks CID Response. In the Canadian lawsuit, the Affidavit of Marc D’Souza sworn March 7, 2007, includes an attachment which confirms that ByteHosting in Cincinnati, Ohio provides “call center vendor services” including customer support and technical support. See Ex. 17, Att. K, at D’Souza Exhibit C.
72. After purchasing AdvancedCleaner on or about March 12, 2008, I posed as a consumer named

“Jessie Logan” and called the phone number (800) 755-5909, which was listed in the onscreen confirmation page for my purchase, in addition to being listed on the credit card statement.

During that call, I spoke with a representative named, “Tina” who gave me the telephone number (800) 430-8969 as the support line for AdvancedCleaner. According to the Junction Networks CID response, both of these telephone numbers are assigned to James Reno of ByteHosting Internet Services, LLC. See Section IV.C for additional information regarding that telephone call.

73. The telephone numbers, (800) 755-5909 and (202) 904-2212 appeared on the homepages for *virussw.com* and *supportsw.com*. These web sites were listed on my undercover credit card statement after purchasing WinAntiSpyware and AdvancedCleaner and the onscreen and email confirmations of my order. Both of these web sites are hosted on the same IP address as *drivecleaner.com*, *winantivirus.com*, *winantispyware.com*, *errorprotector.com*, and *sysprotect.com*, which as previously discussed, have connections to Winsoftware and IMI.
74. The Microsoft CID response included several email messages from *cathy.walton@winsoftware.com* which reference “James” and various toll-free telephone numbers. Her title is listed as “WW CC Manager.” Several messages to *cathy.walton@winsoftware.com* from employees at CRB reference a call center. I believe “WW CC Manager” means “World Wide Call Center Manager” and that this is James Reno’s mother who runs the Defendants’ call center.
75. The Microsoft CID response contained an email dated January 26, 2007 with questions and answers pertaining to consumers who call CRB to complain about a collection account. At the

bottom of the questions and answers, the email read, “James.” I understand this to mean that James composed the questions and answers. One of the questions read, “This is fraud, I’m reporting you too . . .” The answer read:

If you did not place the order we can launch a fraud investigation. To launch a fraud investigation it may require you to file a police report on the alleged fraud charges in which the police will ask you certain questions under penalty of perjury [*sic*] (lying to the cops). If you want to launch a fraud investigation I can set your order to fraud and open a case, generally this process will take 4-6 weeks and can take up-to 2 months before the money is returned.

A true and correct copy of this email message is included as **Attachment T**.

ii. JAMES RENO’S CONNECTION TO THE DEFENDANTS’ SOFTWARE SECURITY PRODUCTS VIA LIMELIGHT NETWORKS

76. On or about October 23, 2007, I downloaded Drivecleaner from <http://cdn.drivecleaner.com> using a VMWare computer in the FTC Internet Lab. Prior to downloading the DriveCleaner file, I activated the network protocol analyzer, Wireshark. See Paragraph 7 for information on Wireshark. At the conclusion of the download, I reviewed the Wireshark log and determined the file was downloaded from the IP address 208.111.153.244. I performed a search on this IP address and determined that the file was downloaded from Limelight Networks, Inc.
77. The Commission sent a CID to Limelight Networks, Inc. (“Limelight”) to determine the subscriber associated with the IP address, 208.111.153.244 during the exact date and time I downloaded DriveCleaner from Limelight’s servers. According to its web site, Limelight Networks provides content delivery networks (“CDN”). A content delivery network allows

users to access a web site more quickly because portions of a site have been copied to servers that are closer to the user's geographic location. In this instance, visitors to the Defendants' web sites are retrieving content via Limelight Networks servers.

78. According to the Limelight Networks CID response, the customer associated with the IP address, 208.111.153.244 is "SetupaHost, Inc." in Ontario, Canada. James Reno is listed as the customer, the sales and billing contact with the email address of *james@setupahost.net* and the telephone number (513) 685-0032 x4501. Included as **Attachment U** is a true and correct copy of the Limelight Networks CID response. On or about May 21, 2008, I performed a search for this phone number using Google, located at *http://www.google.com*. According to the Andersen Area Chamber of Commerce, this phone number is assigned to ByteHosting Internet Services, LLC. The contact is listed as Julia Reno, HR Manager.
79. The same email address that appears in the Limelight CID response, *james@setupahost.net*, is listed as a secondary email contact in the Yahoo! CID response, for *mydomains0@yahoo.com*, used in the registration of *forceup.com*, one of Defendants fake advertising companies. See Paragraph 147.
80. According to the Limelight Networks CID response, the payment for services provided by Limelight was received by wire transfer from a company called "Sunwell Inc." Sunwell in Latvia also paid James Reno more than one million dollars and was used in conjunction with Defendants' fake advertising companies. See Paragraphs 93.
81. The CID response from Limelight Networks included logs of connections to the Defendants' URLs made by consumers to Limelight Networks. The logs included URLs that contained the

names, "Locus Software," "WinantiSpyware," "WinAntiVirus," Winsoftware"
"YourPrivacyGuard," "BestSellerAntivirus," "Winanonymous," "StorageGuardSoft" and
"Safetydownload." See Attachment U.

82. In the Canadian lawsuit, the Affidavit of Marc Gerard D'Souza sworn January 31, 2008, included attachments consisting of accounting spreadsheets. One of these spreadsheets, "Exhibit I," has several entries requested by "James." Some of the entries list the "Beneficiary" as "Dell Marketing" with the "Purpose/Remarks" listed as "server purchase for Toronto." Other entries requested by "James," list the "Beneficiary" as "Limelight Networks" with the "Purpose/Remarks" listed as "servers/bandwidth." See Ex. 17, Attach. L, ¶ 13 and D'Souza Exhibit I at page 191, 201.
83. The US Bank CID Response included several transactions drawn on the ByteHosting account for hotels, food, gasoline, parking, and other expenses in Toronto, Canada which is consistent with the transactions included in Marc D'Souza's affidavit mentioned in the previous paragraph.

iii. RENO'S CONNECTIONS TO OTHER DEFENDANTS

84. Included in the US Bank CID response, were numerous checks paid to Verizon Wireless. The Commission sent a CID to Verizon Wireless to obtain James Reno's cellular telephone records. The call records indicate that James Reno called Defendant Kristy Ross and Kristy Ross called James Reno on several different occasions. See Paragraph 113 for additional information about Kristy Ross' cell phone call records.
85. James Reno worked with Sam Jain at Jain's company, Efront, which was confirmed by a news article from CNET News. See Section III.E for information on Sam Jain. According to an

interview with James Reno, Reno, a high school junior at the time, was the Chief Technology Officer of Efront beginning in March 2001. According to the interview, Reno had been with Efront since 1999 when he worked as webmaster for Bytecenter.com. The domain *bytecenter.com* currently lists ByteHosting Internet Services, LLC as the technical contact in the Whois record. *Bytecenter.com* lists James Reno as the President of ByteHosting Internet Services, LLC.

iv. SETUPAHOST.NET

86. Throughout the course of the investigation, I discovered many connections to a company in Canada called Setup A Host, Inc. with a web site of *http://www.setupahost.net*. On or about November 20, 2007, I used a “clean” VMWare image and started Wireshark before visiting the web site *http://adfarm.mediaplex.com/ad/ck/49725*. When the advertisement appeared, I clicked the button labeled, “hide files” that appeared in the advertisement. I was redirected to another page on *http://www.drivecleaner.com* which included a button labeled, “Download” next to the words “Drive Cleaner.” When I moved my mouse over this button, it read, “*http://cdn.drivecleaner.com/installdrivecleanerstart.exe*” in IE’s status bar.
87. After downloading the DriveCleaner program, I reviewed the log in Wireshark and found a packet that included the URL I had been redirected to at *http://www.drivecleaner.com/freeware/index.php*. The “Destination” this packet was retrieved from was 204.16.207.197. I performed a search on this IP address at *http://www.arin.net* and determined this IP address is associated with Setup A Host in Canada.
88. I also found the packet related to “*/installdrivecleanerstart.exe*.” in the Wireshark log which

indicated it was being downloaded from 208.111.153.244. This IP address is assigned to Limelight Networks. See Paragraph 78 for additional information.

89. The Limelight CID response shows James Reno at “SetupAHost, Inc.” as the customer, sales and billing contact for this IP address and he uses an email address of *james@setupahost.net*. See Paragraph 78. Additionally, the Whois History record for the domain *globedat.com* dated August 11, 2005 shows the domain was registered to “Setupahost” with the telephone number (800) 755-5909, which is assigned to James Reno. See Paragraph 71.
90. The domain *setupahost.net* shares an IP address with several of the Defendants’ security software products, including *drivecleaner.com* and *popupguard.com*. As mentioned in Paragraph 44 above, the security certificate for *popupguard.com* lists “Hosted by Setup A Host, Inc.” in the subject information, with an address in Thornhill, Ontario, Canada. I reviewed at least 20 domains associated with the Defendants that included “Hosted by Setup A Host, Inc.” in the subject information of the sites’ security certificate. Included as **Attachment V** are true and correct copies of screenshots I made of several websites that included “Setup A Host, Inc” in the subject information of the site’s security certificate.

D. BYTEHOSTING INTERNET SERVICES, LLC

91. According to information received from Junction Networks, James Reno and ByteHosting Internet Services, LLC were listed as the customer associated with the phone number (800) 755-5909, among other phone numbers. On or about August 10, 2007, I visited the Ohio Secretary of State’s web site located at *http://www.sos.state.oh.us/*. According to the Ohio Secretary of State, ByteHosting Internet Services, LLC and ByteCenter Web Services, LLC are limited liability

companies registered in Ohio at 3864 McMann Road, Suite A, Cincinnati, Ohio. James Reno is listed as the Agent for both of these companies. Included as **Attachment W** are true and correct copies of the records I obtained from the Ohio Secretary of State's web site.

92. The Affidavit of Marc Gerard D'Souza sworn January 31, 2008, from the Canadian lawsuit, refers to a transfer of funds made to ByteHosting Internet Services, LLC. D'Souza states, "... ByteHosting Internet Services, LLC, an Ohio Corporation owned by James Reno ... that was referred to as the Business's "Ohio Office." See Ex. 17, Attach. L, ¶ 52.
93. According to the statements received from US Bank in response to the Commission's CID, from January 2005 to January 2008, ByteHosting Internet Services, LLC received wire deposits from several companies including Sunwell, Winpayment Consultancy SPC, and others affiliated with IMI. The table below indicates the name of the company from which the wire deposit occurred, the amount deposited, and the grand total.

Name of Company Originating the Wire	Total Amounts Wired to ByteHosting (Jan. 2005 to Jan. 2008)
Sunwell Inc	US \$1,058,564.30
WinPayment Consultancy SPC	US \$722,318.37
WinSecure Solutions	US \$42,250.00
Web Intgtd Net Solutions	US \$33,322.26
GRAND TOTAL	US \$1,859,954.93

ByteHosting Internet Services, LLC received over \$1.8 million from companies affiliated with IMI between January 2005 and January 2008. These wire deposits made up almost 97% of the total deposits made into ByteHosting Internet Services, LLC's account from January 2005 to

January 2008.

94. ByteHosting Internet Services, LLC, received a wire transfer of \$3,500 from an entity called, “Billingnow BV.” As mentioned in Paragraph 42, the site, *popupguard.com* shares an IP address with *billingnow.com*. Also, clicking the link to purchase *popupguard.com* redirected me to a Payment Page residing on *billingnow.com*. In 2003, according to Whois history records, the domain *billingnow.com* was registered to Innovative Marketing, Inc. at 1876 Hutson Street in Belize. See Attachment A. In 2004, the Whois information was changed to a P.O. Box located in Peterborough, Ontario, Canada, which is where Setup A Host, Inc. is located.
95. Marc D’Souza’s Affidavit sworn January 31, 2008, includes an accounting of “all outflows from the D’Souza companies.” Included in this accounting are several entries where “ByteHosting Internet Services LLC” is listed as the “Beneficiary,” “James” is the requestor, and “Sam” is listed in the “Approved by” column. The “Purpose/Remarks” for these entries include, “Payroll/Office Expenses,” payroll taxes, utilities, and rent. See Ex. 17, Attach. L, at D’Souza Exhibit I, at pages 186-187.
96. The documents received from US Bank include copies of checks that were written from ByteHosting’s account. I analyzed the payments made to and from this account and determined that most of the money deposited into the account came from accounts affiliated with IMI, such as Sunwell and Winpayment Consultancy SPC as described in the above chart. See Paragraph 93. There were numerous checks marked with a date range and the words, “Pay Period.” Many of these checks include addresses located in Ohio. I believe these checks to be payroll checks paid to about 40 individuals working for ByteHosting Internet Services, LLC in Ohio including,

“Catherine Walton,” (a.k.a. Cathy Walton), “Julia Reno,” (HR Manager at (513) 685-0032) and “Tina Hughes” (whom I believe to be the “Tina” I spoke with after purchasing AdvancedCleaner. There were also checks written from this account that appeared to be for rent, utilities, computer equipment, and other office related expenses which are consistent with the accounting listed in Marc D’Souza’s affidavit mentioned in the previous paragraph.

E. SAM JAIN

97. As established in this section, Sam Jain is the Chief Executive Officer of Innovative Marketing and was a party in the Symantec lawsuit along with James Reno and Innovative Marketing, Inc., among others. See Paragraph 102.
98. According to the Affidavit of Sam Jain sworn February 19, 2007, from the Canadian lawsuit, Sam Jain has served as the Chief Executive Officer of IMI since approximately July 2002. In early 2002, Kristy Ross introduced him to Daniel Sundin who had already incorporated IMI and the three of them agreed to collaborate on this venture. See Ex. 17, Attach. F, ¶ 1, 3.
99. In the Affidavit of Sam Jain sworn March 6, 2007, Jain attaches a profit and loss statement indicating that IMI grossed more than \$92 million between 2004 and 2006. See Ex. 17, Att. M, ¶ 4.
100. Jain also mentions in this his affidavit sworn February 19, 2007, that “there is a hierarchy for the approval of expenditures within IMI, with Daniel and I having the ultimate authority to approve or reject any request for expenditures of the company’s resources.” See Ex. 17, Attach. F, ¶ 63.
101. The Commission obtained a California driver record for Sam Jain which lists his address as of June 27, 2008, as 355 1st St., 2801, San Francisco, CA 94105.

102. In or about April 2004, Symantec Corporation sued James Reno, ByteHosting Internet Services, LLC, Innovative Marketing, Inc., and Sam Jain for alleged violations of Symantec's intellectual property rights. In the suit, Symantec alleged that Jain and his co-defendants used pop-up ads that misled consumers into believing that their Symantec software was about to expire and needed to be renewed or would not function properly. Reno, ByteHosting, IMI, and Jain allegedly used pop-up ads that redirected unsuspecting consumers to a Web site selling their own software instead of Symantec's. Jain also sent out unsolicited commercial email messages that advertised counterfeit Symantec software at discounted prices using web sites such as *buysmarter.com*. The domain *buysmarter.com* was previously registered to Innovative Marketing at 1876 Hutson Street in Belize, the same address that was used by Daniel Sundin to register domains with TUCOWS. Symantec received a default judgment of \$3.1 million against Jain in this lawsuit. In entering the default judgment the Court found that Jain "cynical[ly] and intentional[ly] manipul[at]ed" the proceedings by evading service of the complaint. Included as **Attachment X** is a true and correct copy of the Complaint and the Order Denying Sam Jain's *Ex Parte* Application for Relief from Default filed in the Symantec lawsuit.
103. According to online news sources, Sam Jain was the CEO of a company called Efront in 2001. On or about September 11, 2008, I queried the California Business Portal at <http://www.kepler.sos.ca.gov>, for information on Efront. I found a record for Efront Media, Inc. filed May 9, 2000 that listed Sam Jain as the registered agent for service of process. Included as **Attachment Y** is a true and correct copy of this record.
104. In or about March 2001, instant messaging logs from Efront were posted on the World Wide Web which discussed business partners, employees and affiliated web sites, including James

Reno and Kristy Ross. James Reno worked at Efront as the Chief Technology Officer. See Paragraph 85. I accessed these instant messaging logs from <http://www.echostation.com/efront> on or about December 3, 2007.

105. These instant messaging logs included a “conversation” between Sam Jain and Kristy Ross. After reviewing this log, it appears that Sam Jain and Kristy Ross were at one point in a romantic relationship.

F. KRISTY ROSS

106. As established in this section, Kristy Ross is the Vice President of Business Development of Innovative Marketing, Inc. and has acted in that role since approximately July 2002. She used a Globedat email address when corresponding with MyGeek regarding the placement of advertisements for Defendants’ software security products. To place these advertisements with MyGeek, she used credit cards in the name of “M D” (which I believe to be Marc D’Souza- See Paragraph 126), “Daniel Sundin,” and wire transfers from IMI’s account in order to pay for these advertisements.
107. According to the Affidavit of Kristy Ross sworn March 6, 2007, from the Canadian lawsuit, she has worked with IMI in the role of Vice President of Business Development since July 2002, although she did not formally hold that title until January 2006. Her responsibilities in that role have included business expansion, sales and marketing and product optimization. She has worked with IMI since early 2002. See Ex. 17, Attach. J, ¶ 1.
108. According to the Affidavit of Daniel Sundin sworn February 19, 2007, in the Canadian lawsuit, Sundin suffers from a medical condition that sometimes makes it difficult to perform some of his

duties at IMI. Sundin states, “some of my duties have been assumed from time-to-time by Kristy, who I consider to be a savvy manager and technically knowledgeable in my areas of computer software and design as well as marketing skills.” See Ex. 17, Attach. G, ¶ 15.

109. Included in the Microsoft CID response are screenshots of account profiles that were set up in connection with advertising campaigns for Defendants’ products and services with MyGeek. Most of these profiles list either “Kristy Ross” or “K R” with the company name, “Globedat” and the email address, *marketing1@globedat.com*. The telephone number listed with these accounts is (206) 730-2606. Although many of the screenshots list an address in Seattle (which is consistent with the telephone number provided), for some of the profiles she lists P.O. Box 54838 in Manama, Bahrain. Included as **Attachment Z** is a true and correct copy of a chart created by MyGeek which displays the profile information, the amount of money spent on each advertising campaign and the number of impressions and payment information related to Daniel Sundin.
110. Throughout the documents from MyGeek, Kristy Ross discusses the placement of advertisements for the following IMI products: *drivecleaner.com*, *winantivirus.com*, *errorsafe.com*, *errorprotector.com*, and *systemdoctor.com* among others. Included as **Attachment AA** are true and correct copies of two email messages regarding Defendants’ software security products and Innovative Marketing.
111. According to emails between Kristy Ross and MyGeek produced as part of the Microsoft CID response, Kristy Ross used Daniel Sundin’s credit card in order to pay for advertisements relating to ErrorProtector, SystemDoctor, ErrorSafe, WinAntiVirus, and DriveCleaner. She also

used international bank wires originating from an account called “Innovative Marketing” to pay for some of these advertisements. See Attachments Z and AA. Ross also used credit cards in the name of “M D” which as discussed below in Paragraph 126, I believe to refer to Marc D’Souza. In total, Kristy Ross placed \$3.3 million of advertisements for Defendants’ products with MyGeek. See Attachment Z.

112. In most of this correspondence with MyGeek, Ross uses *kristy@globedat.com* as her email address when discussing advertising campaigns such as *winantivirus.com*, *drivecleaner.com* and *winfixer.com*. She also lists her cell phone number which uses a 206 Seattle area code in the account profiles. See Attachment Z. As previously discussed, the domain *globedat.com*, was previously registered to “Setupahost” and listed one of James Reno’s telephone number, (800) 755-5909. See Paragraph 89.
113. The Commission sent a CID to Sprint to obtain Kristy Ross’ cellular telephone records, which list her cell phone number with a Seattle, WA area code of 206. This telephone number was the same number that Kristy Ross listed in the email correspondence with MyGeek. The call records indicate that Kristy Ross called Defendants James Reno and Marc D’Souza. According to the call records, between April 2006 and November 2007, Kristy Ross called Defendant Marc D’Souza and Globedat at (416) 836-6838 about 230 times. The Microsoft CID response includes credit card authorization forms in which Marc D’Souza lists (416) 836-6838 as the phone number for Globedat. Kristy Ross also called the telephone number (513) 797-1317 more than 25 times between July 2005 and April 2006. I performed a search in Lexis Nexis’ Law Enforcement Solutions database in or about June 2008 and determined that (513) 797-1317 was previously associated with ByteHosting Internet Services, LLC.

114. In or about August 2006 Kristy Ross provided a Walkersville, Maryland address to MyGeek. The Commission obtained a copy of Kristy Ross' driver's license record, issued on January 28, 2008, which lists the same Walkersville, Maryland address.
115. On multiple occasions, MyGeek informed Ross that the advertisements, including for WinFixer, she had placed were generating complaints from their partners due to the advertisements attempting to auto-download software and force consumers to view Defendants' web sites. MyGeek informed Ross that these advertisements were not allowed on their network and needed to be fixed or removed. Although Ross promised to resolve the problems, they continued to occur. Included as **Attachment BB** is a true and correct copy of these email messages.
116. One of MyGeek's advertisers, NetBlue, complained to MyGeek about Ross' Winfixer advertisements, "I just went to the test link and got the winfixer ad again, and that thing is an aggressive and bad ad- I do not want [sic] that campaign running on our users at this point- the ads are too aggressive." Included as **Attachment CC** is a true and correct copy of these email messages.
117. On several occasions, MyGeek informed Ross that its advertising partners would not run advertisements for antivirus or antispyware software. Ross replied, on January 24, 2006, that she could offer a product that guarantees not to remove their adware. Again, on September 1, 2006, Ross received an email from a MyGeek representative that indicated that their partners do not want to run "spyware removal, registry cleaner, anti-virus" advertisements. Kristy Ross replies that the reason they do not want to run, "antivirus, etc is [sic] because they are Spyware/Adware companies." She then says, "we are 100% able to keep their product OUT of

the database if they are willing to run the advertisements. You might also consider presenting that. I can do it with all the software sources we run.” Included as **Attachment DD** is a true and correct copy of this email message.

118. In an email dated March 29, 2007, MyGeek informed Kristy Ross that the company “will no longer be running ads from any advertiser that sell products in the area of spyware, antivirus, registry cleaner, system doctor, evidence eraser, and the like” because their relationships with “traffic partners have been threatened and we just can't afford the risk any longer.” In response, Ross stated that her company has “spent well over a million dollars with your company “and they have “500 [other] advertising deals.” Included as **Attachment EE** is a true and correct copy of this email message.
119. As discussed in Paragraph 105, it appears that Kristy Ross and Sam Jain were once involved in a romantic relationship.

G. MARC G. D’SOUZA

120. As established in this section, Marc G. D’Souza acted as the Chief Financial Officer and Chief Marketing Officer of Innovative Marketing. Credit cards listing “M D” and “M D’Souza,” which I believe to be Marc D’Souza’s, were used to purchase advertisements for Defendants’ software security products. He and his father, Maurice D’Souza (see Section III.H), set up payment processing facilities for Defendants’ software security products.
121. The Canadian pleadings list an address for Marc G. D’Souza in Toronto, Canada and his Counterclaim states he is Canadian citizen. See Ex. 17, Attach. B, ¶ 18. In many of the documents I reviewed during the course of the investigation, Marc D’Souza used addresses and

telephone numbers located in Ontario, Canada when doing business on behalf of IMI and its affiliates.

122. According to his Counterclaim, Marc G. D'Souza began working with IMI in or around January 2002. He terminated his relationship with IMI on or about December 31, 2006. See Ex. 17, Attach. B, ¶ 18. This is confirmed in the Claim, which states that Marc D'Souza stopped working for IMI in December 2006. See Ex. 17, Attach. A, ¶ 3.
123. Marc D'Souza learned about a "scanner approach" to market Defendants software security products and encouraged Jain to adopt this technique. In or about June 2005, Defendants began marketing "Winfixer" using the "scanner approach." See Ex. 18, Att. B, ¶ 166-168.
124. According to his Further Fresh as Amended Statement of Defence and Counterclaim of the Defendant Marc Gerard D'Souza, D'Souza considered himself the Chief Marketing Officer. See Ex. 17, Att. D, ¶ 158. He also acted as Chief Financial Officer by establishing the relationships with the banks that provided merchant account processing for Defendants' software security products. See Ex. 17, Attach. D, ¶ 17, 142-144, 148, 153-154. The Further Fresh Counterclaim also states,

By establishing and managing most of the merchant account processing facilities, Marc had de facto control over most of the Business' funds . . . he was the partner in charge of controlling the Business's finances in order to minimize tax and legal liabilities for the Business. See Ex. 17, Attach. D, ¶ 18-19.

125. According to both the Counterclaim and the Further Fresh Counterclaim, IMI was having difficulty maintaining relationships with credit card payment processors due to the high numbers of consumer complaints and chargebacks. See Ex. 17, Attach. B, ¶ 81-82. Marc D'Souza and

his father, Maurice, therefore used their relationships with merchant banks overseas to establish payment processing via banks in Toronto and throughout the Middle East for Defendants' software security products. See Ex. 17, Attach. D, ¶ 141, 143-144.

126. Included in the Microsoft CID response were MyGeek documents in which several customer profiles listed "M D" as the name and the email address, *marketing2@globedat.com*. These profiles listed Kristy Ross' cell phone number and P.O. Box 54838 in Manama, Bahrain, which Kristy also uses in several profiles listing her name. The company names in the profiles connected with "M D" are listed as "Antivirus" and "Globedat." Additionally, there is a profile that reads "M Dsouza" with an address of 22 Carnegie Crescent in Thornhill, Ontario, Canada. This is the same address listed in the security certificate for *popupguard.com* on the billing page, *billingnow.com*. I believe "M D" and "M Dsouza" were used by Marc D'Souza to sign up for the MyGeek account profiles. See Attachment Z.
127. The two billing sites that were listed on my undercover credit card statements after my purchases of WinAntiSpyware and AdvancedCleaner are both associated with Marc D'Souza. *Virussw.com* is registered to Synergy Software B.V. which, according to the Counterclaim, is a company owned by Marc D'Souza and operated out of the Netherlands. This domain shares an IP address with *supportsw.com*.

H. MAURICE D'SOUZA

128. Throughout the pleadings from the Canadian lawsuit, Marc D'Souza discusses his father, Maurice D'Souza, and the role Maurice played in IMI. As previously stated, according to both the Counterclaim and the Further Fresh Counterclaim from the Canadian lawsuit, IMI was

having difficulty maintaining relationships with credit card payment processors due to the high numbers of consumer complaints and chargebacks. Maurice D'Souza became involved with IMI when he and Marc D'Souza used their relationships with merchant banks overseas to establish payment processing for Defendants' software security products. See Ex. 17, Att. D, ¶ 143-145.

129. According to the Affidavit of Marc D'Souza sworn February 20, 2007, from the Canadian lawsuit, Maurice D'Souza is a citizen of Ontario, Canada, residing in Thornhill, Ontario. See Ex. 17, Attach. H, ¶ 66-67.
130. The Claim in the Canadian lawsuit states that "Maurice has never been directly employed by IMI, nor is he a party to any agreement with IMI that would allow him to receive funds from it." See Ex. 17, Attach. A, ¶ 4.
131. Marc and Maurice D'Souza control millions of dollars from the sales of IMI's software security products. According to the Affidavit of Marc Gerard D'Souza sworn January 31, 2008, in the Canadian lawsuit, "approximately US \$40,000,000 of proceeds of the Business [is] held in bank accounts of the D'Souza Companies and bank accounts and assets of the D'Souzas personally. See Ex. 17, Attach. L, ¶ 118. According to the Affidavit of Sam Jain sworn February 19, 2007, in the Canadian lawsuit, approximately \$18 million of IMI's money went into accounts in Maurice's name. See Ex. 17, Attach. F, ¶ 67.
132. Maurice's resume, included as part of the Affidavit of Sam Jain sworn February 19, 2007, in the Canadian lawsuit, lists Maurice working for Web Integrated Net Solutions, the company that received payments from the Defendants' collection agency, CRB. See Ex. 17, Attach. F, ¶ 46 and at Jain Exhibit W. This company also paid over \$33,000 to ByteHosting Internet Services,

LLC. See Paragraph 93. Maurice D'Souza lists his role in this company as "heavily involved in all aspects including product developments, consulting, pricing, distribution and marketing."

133. The resume also lists Maurice D'Souza as working for Billingnow.com Inc., Winpayment Consultancy and Billing Solutions. See Ex. 17, Attach. F, ¶ 46 and at Jain Exhibit W. Winpayment Consultancy paid ByteHosting Internet Services, LLC over \$700,000. Billingnow also made wire transfers to ByteHosting Internet Services, LLC and *billingnow.com* shares an IP address with web sites for Defendants' software security products in addition to previously being registered to Innovative Marketing in Belize.
134. Marc D'Souza states in his Counterclaim from the Canadian lawsuit that Maurice, "provided critical financial services to the Business and ensured its survival." See Ex. 17, Attach. B, ¶ 19. In the Further Fresh Counterclaim from the Canadian lawsuit, he stated that from April 2004 until December 2006, "[Maurice's] services consisted of the creation and maintenance of merchant account processing facilities, tax sheltering, financial management of the Business's retained profits, corporate structure planning, management of payments to vendors and suppliers and management of internal expenses of the Business." See Ex. 17, Att. D, ¶ 145.
135. Marc D'Souza states in the Further Fresh Counterclaim from the Canadian lawsuit that almost all of the Business's merchant accounts were being managed by Marc and/or Maurice and these accounts were used to pay the Business' vendors "with Marc, Jain and Sundin's knowledge and approval." See Ex. 17, Attach. D, ¶ 144.
136. In Marc D'Souza's affidavit sworn February 20, 2007, he states several facts about his father's involvement and the accounts used to control funds. For example, he indicates that Sam Jain

knew of Maurice's role and that personal accounts were used in conjunction with business accounts, "He [Sam Jain] knew where and why my father had set up DSouza Management Companies. He similarly knew at all times how much money was in any of the D'Souza Companies' accounts, and in fact had electronic access to many of the D'Souza Companies' operating accounts. Also, if and when monies were transferred to personal accounts of either my father or myself, he knew what amounts had been transferred and why and, in fact, was in ostensible agreement with all these transfers." See Ex. 17, Attach. H, ¶ 35.

I. ATTEMPTS TO HIDE IDENTITY

137. Throughout the course of the investigation, I visited Defendants' web pages and associated Whois results, reviewed the Defendants' advertisements, purchased Defendants' products, researched the Defendants and their companies, analyzed consumer complaints, and other related tasks. Discussed below is an analysis of the Defendants' attempts to hide their identities and make it difficult for consumers to obtain refunds and/or locate and contact the company, including but not limited to: providing false or incomplete Whois information, using third party likenesses and trademarks, numerous (and sometimes fake) telephone numbers, email accounts, and/or other contact details, multiple credit card merchant identifiers, and using foreign or fake company names that do not have official records.
138. The section below will also include specific references to pleadings from *Innovative Marketing, Inc. v. Marc Gerard D'Souza et al.* in which Defendants discuss some of the techniques they used to hide their identities and their attempts to evade law enforcement.

i. FAILURE TO MAINTAIN CORPORATE FORMALITIES

139. Innovative Marketing, Inc. did not adhere to corporate formalities with respect to business structure, the titles and roles of Officers, or business records. This is confirmed throughout the pleadings in the Canadian lawsuit. The Further Fresh Counterclaim states,

[The Business] relied on convoluted, complex, and [an] opaque business structure[] designed to confuse customers and regulators as to the identity of the true owners and operators of these ventures and to minimize tax liability for the principals. The partners and the corporations under their control relied on few or no written documents to record the partnership's activities; revenues earned by the ventures ended up in different corporate accounts; the partners had no formal, written partnership agreement and deliberately did not keep formal records of the partnership's activities. See Ex. 17, Att. D, ¶ 6.

140. The Further Fresh Counterclaim in the Canadian lawsuit also indicates that IMI,

[W]as merely one of many corporate and unincorporated entities that contributed technical and support services to the partnership. Marc, Jain, and Sundin each exercised independent control of numerous corporations and unincorporated entities that made contributions of technical, support, financial and marketing services. See Ex. 17, Attach. D, ¶ 8.

141. IMI officers used informal methods of communication and documentation as discussed in the Further Fresh Counterclaim in the Canadian lawsuit:

At all material times, Marc, Jain and Sundin communicated through informal channels such as instant messages and e-mails. There was little or no formal documentation to support major decisions made by the Business. The need for formal documentation was ignored by all of the partners” See Ex. 17, Attach. D, ¶ 72.

* * *

[F]ew decisions were recorded in formal agreements or documents, and very few documents were created to record the details of the complex relationships between the

corporations and unincorporated entities that held the Business's assets.

See Ex. 17, Att. D, ¶ 165.

142. Additionally, in regard to titles of the officers, the Further Fresh Counterclaim in the Canadian lawsuit notes “[t]hese descriptions did not correspond to formal titles within the Business, as there were none, [but titles that were used were] merely intended to explain to the [Innovative Marketing Ukraine] staff who was responsible for particular issues.” See Ex. 17, Attach. D, ¶ 158.

ii. USE OF FALSE, INCOMPLETE, OR INCORRECT INFORMATION

143. The Defendants have used several different addresses, many located throughout the world to register their web sites. There is little consistency among the Whois records which made it difficult to determine which sites were operated by the Defendants. Several of the Whois history records show changes in the registration information throughout the last several years as the Defendants repeatedly changed the Whois information including the names, company names and addresses that appeared in the Whois records. The Defendants often only listed the software product's name as the registrant company and contact information could not be found on most of the web sites. In many of the Whois results, the telephone number for the registrant was listed as (555) 123-1234. Additionally, there are several domains that have changed IP addresses throughout the course of the investigation. See Attachments A and H.
144. In some instances, Defendants used a proxy or privacy service (often ones located in the Netherlands, Brazil, or Canada) to register many of their web sites. This shields their identity from the general public and law enforcement. I reviewed Whois and Whois history records for

forceup.com, innovativemarketing.com, dataconfidentiality.com, multimediafixer.com, pcsupercharger.com and *malwarecrush.com* which all used privacy or proxy services. See

Attachment A.

145. In many of the Whois registrations there were generic email addresses, often *hostmaster@[productname]* and the web sites would list *support@[product name]*. In Whois results, Defendants commonly used free email addresses from Yahoo! such as *no_name_inc@yahoo.com* which did not identify a company or individual.
146. The Commission sent a CID to Yahoo! for information on the identity of those email account holders. In most cases, the registration information came back with little or no relevant information, often just a country or zip code but no actual contact name, telephone number or full address. One of the email addresses for which the Commission requested information from Yahoo! was *no_name_inc@yahoo.com*. The IP logs received from Yahoo! include several log-ins from the IP address 194.140.237.200, which is associated with Innovative Marketing Ukraine. This email address was listed in the Whois record for *drivecleaner.com* which Daniel Sundin lists as an IMI product web site in the Claim in the Canadian lawsuit. See Paragraph 46. Included as **Attachment FF** is a true and correct copy of the Yahoo! CID response pertaining to *no_name_inc@yahoo.com* and the IP information for 194.140.237.200.
147. The Whois information for *forceup.com*, one of the advertising companies that placed ads for Defendants' software security products, listed *mydomains0@yahoo.com*. See Paragraph 161 below for additional information. The registration information for this email account listed "Mr. Master hostmaster" in India but included an alternate email address of *james@setupahost.net*.

This is the same email address that was used by James Reno for the account at Limelight Networks. Included as **Attachment GG** is a true and correct copy of the Yahoo! CID response pertaining to *mydomains0@yahoo.com*.

148. According to Marc D'Souza's Counterclaim in the Canadian lawsuit,

domain registration information was modified to conceal the identity of the true operators of the Business. In addition, domain registration information was frequently changed to confuse the public and shield the Business from liability. In fact as the Business grew, detailed policies were established to provide maximum anonymity in the registration, operation and administration of the Business' domains. The domains themselves were used for a short period of time and then discarded or abandoned when there were too many customer complaints or complaints from individuals and security companies who encountered the aggressive or misleading advertising. See Ex. 17, Att. B, ¶ 107.

149. The Counterclaim in the Canadian lawsuit also states, "Names of fake entities were used, usually corresponding to the domain name . . . In many cases the Business' products and services themselves were claimed to be owned by fake companies in the name of the product itself." The Counterclaim also states that obscure addresses, such as in Pakistan, were used in the domain registrations. See Ex. 17, Att. B, ¶ 107.

150. The Defendants formed fake advertising companies, such as NetMediaGroup and BurnAds to place advertisements for their software security products with various web sites including *zillow.com*. Payments for some of these advertisements came from the Sunwell bank account. The names and addresses given for these companies was often foreign. See Paragraph 161 below for additional information on the fake advertising companies.

iii. INTERNATIONAL PRESENCE

151. Most of the Defendants' companies and DBAs are international entities. Therefore, I could not

locate official records for a majority of the companies and DBAs being used by the Defendants. This also made it difficult to identify the individuals behind the security software products and web sites that consumers were complaining about since it was difficult to determine officers of these companies. Company names were often used interchangeably, with the same individuals doing business in multiple companies, with multiple email addresses.

152. According to the Counterclaim in the Canadian lawsuit, IMI used several different names to conduct business:

The Business also used Web Integrated Net Solutions Inc., a British Virgin Islands corporation, Winpayment Consultancy, a Bahrain corporation, Billingnow.com, an Ontario Corporation and WinSecure Solutions, a Singapore corporation and many of the other corporate defendants to represent itself to third parties. New business conducted after January 2004 was carried out in the names of these corporations or GlobeDat. See Ex. 17, Att. B, ¶ 5.

153. Many of the banks utilized by the Defendants are also located overseas. The credit card statement for my purchase of WinAntiSpyware listed Palma Mallorc, which I understand to mean “Palma, Mallorca” a city in Mallorca, located off the coast of Spain. The credit card statement for my purchase of AdvancedCleaner shows a foreign currency charge and lists “ES” which I understand to mean “España,” or Spain.
154. During the course of the investigation, the Commission learned about several bank accounts and credit cards used by the Defendants that are located overseas. For example, one of the credit cards used by Daniel Sundin to pay for domains with TUCOWS was a Swedish credit card. A Canadian credit card in the name of Marc D’Souza was used to pay for advertisements placed with MyGeek. Sunwell in Latvia paid James Reno more than one million dollars and was used

in conjunction with Defendants' fake advertising companies. See Paragraphs 93 and 161.

155. According to the Claim and Counterclaim in the Canadian lawsuit, several relationships were established with banks overseas, such as in Dubai, for processing credit card payments from Defendants' web sites. The Counterclaim states, "the Business maintained a variety of different e-mail accounts, a variety of identities (some real, some fake), and bank accounts in order to confuse, and misdirect customers, suppliers and vendors." See Ex. 17, Att. B, ¶ 107.
156. Defendants had numerous merchant identifiers that were used with credit card companies. These merchant identifiers were used interchangeably. For example, *virrusw.com* and *supportsw.com* were both used in conjunction with my undercover purchase of WinAntiSpyware.
157. Most of the products' web sites did not include company contact information, but instead the "Contact Us" links usually lead to an email form that could be electronically submitted. When company names were listed, I was not able to find corporate information on these entities and the addresses listed on the pages were often foreign.
158. The purposeful use of international resources to confuse consumers and evade law enforcement is confirmed in the Counterclaim in the Canadian lawsuit,

The Business' offshore presence allowed it to escape regulation from the Federal Trade Commission and avoid State Attorneys who were sanctioning and shutting down similar organizations, as well as other civil liabilities from tens of thousands of dissatisfied end consumers. Additionally, the Business started to target people outside of the United States. See Ex. 17, Att. B, ¶ 125.

IV. EVIDENCE OF THE DEFENDANT'S DECEPTIVE PRACTICES

A. ADVERTISEMENTS, "SCANNERS," AND FAKE ADVERTISING COMPANIES

159. Throughout the course of the investigation, I used Google to research the companies, software security products and other information related to the Defendants, their companies, and their advertisements.
160. Among the web sites I reviewed as a result of these Google searches were numerous reports of users being redirected to Defendants' software security product web sites. Some of the web sites users reported being redirected from were Major League Baseball (*mlb.com*), National Hockey League (*nhl.com*), The Economist Magazine (*economist.com*), the National Association of Realtors (*realtor.com*), *zillow.com*, and *e-harmony.com*. Most of the users did not know how they arrived at Defendants' web sites. Among the web sites I reviewed that contained these reports were news sources, online complaint forums that discuss spyware and other computer issues, web sites of companies that manufacture anti-spyware products, and web sites that discussed online advertising.
161. One of these sources I reviewed during the course of the investigation was a web site about spyware in which the author had tracked malicious URLs that directed users to Defendants' software security product sites. This web site is located at <http://msmvps.com/blogs/spywaresucks> ("Spywaresucks"). On numerous occasions, the author of Spywaresucks analyzed the Defendants' advertisements. According to Spywaresucks and other web sites I reviewed, some of the web sites and companies that consumers were re-directed through were: *adtraff.com* (AdTraff), *burnads.com* (BurnAds), *blessedads.com* (BlessedAds),

netmediagroup.net (NetMediaGroup), *forceup.com* (ForceUp), *infyte.com* (Infyte) and *uniqads.com* (Uniqads) I visited several of these domains and found web sites indicating that these companies are Internet advertising companies. This is further confirmed by the Chad Cohen declaration. See Exhibit 14 in which he establishes that NetMediaGroup was identified as the source of Defendant's malicious advertisements on *zillow.com*.

162. On or about December 10, 2007, I performed a reverse IP search for *netmediagroup.net* and discovered that *adtraff.com*, *burnads.com*, *blessedads.com*, *netmediagroup.net*, *forceup.com*, *infyte.com*, and *uniqads.com* all share an IP address with *pcsupercharger.com* (named as an IMI web site in the Defendants' Claim in the Canadian lawsuit) and *errordigger.com*, which in October 2008 shared an IP address with *advancedcleaner.com*. See Attachment H.
163. The Whois information for the domain *forceup.com* lists the email address *mydomains0@yahoo.com*. As previously discussed, *james@setupahost.net* is listed as a secondary email contact for *mydomains0@yahoo.com* in the records the Commission received from Yahoo! CID response. See Paragraph 147.

i. ADVANCEDCLEANER "SCANNERS" AND ADVERTISEMENTS

164. AdvancedCleaner is one of the Defendants' software security products. *Advancedcleaner.com* is on the same IP address as *pcsupercharger.com*, which is listed by Daniel Sundin as an IMI product in his affidavit sworn February 19, 2007. See Ex. 17, Att. G, ¶ 9. *Advancedcleaner.com* was previously hosted on the same IP address on which *drivecleaner.com*, *winantivirus.com*, *systemdoctor.com*, *virussw.com*, *supportsw.com*, and *errorprotector.com* are currently hosted. The web sites, *supportsw.com* and *virussw.com*, associated with my undercover purchase of

AdvancedCleaner, are registered to Synergy Software BV, Marc D'Souza's company according to the Counterclaim in the Canadian lawsuit. After completing the undercover purchase of the product, I called the support line (see Section IV.C) at (800) 755-5909, which the Junction Networks CID response confirmed is assigned to James Reno. I was also given another phone number that is assigned to James Reno while speaking with the customer support representative.

a. REVIEW OF ADVANCEDCLEANER ADVERTISEMENTS

165. One method I used to review advertisements for Defendants' security software products was a review of consumer complaints. I reviewed several complaints about Defendants' software security products that were submitted to the FTC's Consumer Sentinel complaint database (see Section II.B(iv) for additional information on consumer complaints) in which consumers cut and pasted a link to an advertisement they were complaining about.
166. One of the complaints, filed by Joe Renteria (see Exhibit 9, Declaration of Joe Renteria), listed a link to an advertisement for a software security product called AdvancedCleaner. On or about March 11, 2008, I used a VMWare machine in the FTC's Internet Lab to review this advertisement. The link read, *http://advancedcleaner.com/.cleaner/?p=1013&ida=swp_gronexx51&led=2822&afr=pp_2248501152*.
167. Upon visiting the link, a window appeared that looked like a file menu in the Windows operating system. The title of the window read, "Windows" and across the top, it said, "Now performing internal files scan . . ." with a bar showing the "scan progress." Beneath the bar were four sections: "Details," "Scan Results," "Commit Charge (K)," and "Kernel Memory (K)." The numbers listed next to the items in each of these sections increased as the "scan" progressed. On

the left side, it read, "Threats observed" and showed file folder icons, like those used by the Windows operating system. As the "scan" progressed, file folders that included labels such as "Application Data" and "My Documents" appeared. The file folders displayed graphic depictions and photographs of sexual activities. In my experience, this "scan" looked similar to software scans used by the leading antivirus and antispyware programs. At the bottom right of the window was a button labeled, "Remove all."

168. When the "scan" had finished, the message at the top that had read, "Now performing internal file scan . . ." changed to a flashing red message that read, "Illegal porn content found on your PC!" See Sections IV for additional information on AdvancedCleaner, including the free "scanner," the purchase I made and calls placed to the support line. A true and correct copy of this AdvancedCleaner advertisement is included as **Attachment HH**. I created this printout using the procedure described in Paragraph 8.
169. In addition to the AdvancedCleaner advertisement described above, I also viewed several other AdvancedCleaner advertisements. To view these advertisements, I typed in the first part of the URL that I had extracted from the consumer complaint, *<http://advancedcleaner.com/.cleaner/?p=1013>* and substituted the number 1013 for other numbers, such as 1004, 1017, and 1020. Similar to the other advertisements listed in the Renteria's complaint, these advertisements indicated that there were adult, illegal, and/or sensitive files found on my computer, even though I had not visited any web sites that contained such material and I had used a "clean" VMWare computer to visit these advertisements. Many of these advertisements included graphic depictions and photographs of sexual activities and sexually explicit sounding URLs the browser had supposedly visited. The advertisements, when

viewed moments apart on the same machine, found different and conflicting numbers of threats. Included as **Attachment II** are true and correct copies of additional AdvancedCleaner advertisements that I viewed. The FTC Internet Lab's IP address has been redacted in these advertisements.

b. MISREPRESENTATIONS IN ADVANCEDCLEANER ADVERTISEMENTS

170. On multiple occasions I viewed the advertisement for AdvancedCleaner mentioned in the previous section from the consumer complaint, from both a VMWare machine and a separate standard FTC Internet Lab computer. Regardless of which type of computer I viewed the advertisement from it looked identical, including the number of "illegal" files.
171. Every time I viewed the advertisement, along the left side of the advertisement it read, "Threats observed" and showed file folder icons, like those used by the Windows operating system. These folders included the labels, "Application Data," "Cookies," "Local Settings" and "My Documents." The file folders displayed graphic photographs of sexual activities in each folder in the same way Windows indicates which files are contained in the folder. Across the top of the advertisement, it read, "Illegal porn content found on your PC!"
172. On or about October 20, 2008, when I viewed this advertisement on a "clean" VMWare machine, I first opened "My Computer" and chose to display all hidden files and folders in the "View" tab of the "Folder Options." I then visited each of the folders that were listed along the left side of the advertisement by opening "My Computer" and browsing to the folder with the corresponding name as those depicted in the advertisement.
173. I also opened "My Computer" and used the "Search" feature to look for any photo, music and

movie files located on the hard drive of the computer.

174. Using Internet Explorer, I reviewed the source code for this page. I searched for a file with the extension “.swf” which showed a link to an Adobe Flash file located on one of the Defendant’s web sites. To verify that this Adobe Flash file was the source of the advertisement displayed on the screen, I cut and pasted the URL for the Adobe Flash file into a new browser window. The same advertisement appeared on the screen when I entered the location of the Adobe Flash file as when I entered the URL from Joe Renteria’s complaint.
175. I concluded this advertisement was false for several reasons. First, I was using a “clean” VMWare machine, which did not contain adult content or malicious files. See Paragraph 6. Second, each time I viewed this advertisement, no matter what type of computer I was using, the number of objects found in each category were the same. Third, I could not find any files that appeared to be adult content in any of these folders listed in the advertisement. In fact, in this instance, many of the folders contained little or no content because I was using a “clean” VMWare machine. Fourth, I found that although the advertisement indicated it had found 146 Adult pictures and 21 Porn Movies, my search for photo, music, and movie files only located 13 files, all of which were sample files included with the Windows operating system or evidence files I had just created while reviewing this advertisement. Fifth, as discussed in the previous paragraph, I was able to verify the “scan” displayed on the page was actually an Adobe Flash file.

ii. WINANTIVIRUS “SCANNERS” AND ADVERTISEMENTS

176. The software security product, WinAntiVirus is associated with the Defendants. This is

confirmed by Daniel Sundin's affidavit sworn February 19, 2007, from the Canadian lawsuit which lists *winantivirus.com* as an IMI product. See Ex. 17, Att. G, ¶ 9. This site is also listed in the TUCOWS CID response as belonging to the reseller Vantage Software, Daniel Sundin's company. According to Whois history records, *winantivirus.com* was previously registered to Innovative Marketing, Inc. in Belize and a post office box in the Ukraine, the country where IMI's headquarters is located. Defendant Kristy Ross placed advertisements with MyGeek on behalf of IMI for WinAntiVirus and *winantivirus.com* was also included in the log of connections in the Limelight CID response. Consumer complaints list phone numbers assigned to James Reno for WinAntiVirus and *winantivirus.com* lists "Hosted by Setup a Host, Inc." in the subject information of the site's security certificate.

177. Many of the ads I reviewed for WinAntiVirus were on the domain, *amaena.com*. Most of these URLs were in the format, <http://www.amaena.com/securitywormxx/index.php?ax=1&ex=2&h=xx> where xx is equal to a number. I substituted the numbers that appeared for xx in this URL for other sequential numbers and discovered additional advertisements residing on the *amaena.com* web site that were similar to the other ones I had previously reviewed. Included as **Attachment JJ** are true and correct copies of printouts of advertisements I reviewed on *amaena.com*. I created these printouts using the procedure described in Paragraph 8. The FTC Internet Lab's IP address has been redacted in these advertisements. The web site *amaena.com* was registered to IMI in Belize according to Whois history records in 2005. The web site currently is registered to a post office box in the Ukraine, which it has been registered to since 2005. In both the historical and current Whois information for this domain and other security product domains listing IMI, the telephone number 555-123-1234 appears.

178. On or about October 30, 2008, I used Google to search for online complaints about *amaena.com*. I found several forums in which consumers complained about being redirected to *amaena.com* and Defendants software security products appeared. Included as **Attachment KK** are true and correct copies of the relevant portions of two of these online complaints.

a. REVIEW OF WINANTIVIRUS ADVERTISEMENTS

179. Using a standard computer in the FTC Internet Lab, on or about May 11, 2007, I visited one of the advertisements for WinAntiVirus located at <http://www.amaena.com/securityworm555/index.php?ax=1&ex=2&h=10>. This advertisement read, "WARNING! Virus threat detected" and indicated that "Infection detected: W32.ZOTOB.C@mh." The advertisement stated that a remote computer had gained access to my computer and the threat was "SEVERE." Along the left side of this advertisement were "Resources" listed in a bulleted format. This advertisement claimed the solution to the detected threat was WinAntiVirus. At the top of the page, it read, "Security Center Help protect your PC" with a small shield to the left. Included as part of **Attachment LL** is a true and correct copy of this advertisement.
180. On or about May 11, 2007, I visited the URL located at <http://www.amaena.com/securityworm81/index.php?ax=1&ex=2&h=19> on a standard FTC Internet Lab computer. The advertisement indicated that it has detected a virus named, "TrojanSPM/LX." The advertisement further stated the virus, "accesses the affected PC, steals and damage [*sic*] private information inside" and warned, "You have to erase the malware immediately!" It then read, "You have to download one of the latest security solutions to clean

up detected virus. Choose a product and click 'Download' to proceed." Two of the Defendants' software security products, "WinAntiVirus Pro 2007" and "WinAntiSpyware" offer "scans" to remove the virus. These products are both sold by the Defendants. Included as **Attachment MM** is a true and correct copy of this advertisement.

181. On or about November 20, 2007, I visited the URL located at <http://www.amaena.com/securityworm13/index.php?ax=1&ex=2&h=19> using a "clean" VMWare computer. Across the top of this advertisement it read, "WARNING: YOUR CURRENT ANTIVIRUS PROTECTION IS NOT EFFECTIVE!" Beneath this text, it stated, "Your system is currently sending private information and documents to a remote computer. One of these processes (winres32.exe) has just sent us the following information" and included a list of file locations such as "\Windows\System32." Below this text it read, "WARNING: YOUR PRIVATE INFORMATION IS EXPOSED." Towards the middle of this advertisement it read, "System Security Status: CAUTION," and along the top right corner of the ad, it read "Internet Security Center." In the left top corner the words, "Recommended Software: WinAntiVirus Pro2006" were displayed. Along the bottom and the left side were additional solutions such as "WinAntiSpyware 2006," "WinFireWall," and "WinPopupGuard." Several of these software security products can be purchased on winsoftware.com. I re-visited this advertisement from a standard FTC Internet Lab computer on or about November 21, 2007. When I clicked on the "X" button to close out of this advertisement, I observed a new pop-up dialogue box. It read, "NOTICE: You have not completed the scan. There is a security vulnerability from the Serwab. We recommend you DOWNLOAD one of the security software programs to prevent malware infections." There were buttons labeled, "OK" and "CANCEL" below this text. This

advertisement is included as the first page of **Attachment JJ**.

b. MISREPRESENTATIONS IN WINANTIVIRUS ADVERTISEMENTS

182. The advertisement described in the previous section which listed “Infection detected: W32.ZOTOB.C@mh” looked similar to the Windows XP Security Center which is part of the Windows XP operating system. Windows XP Security Center runs automatically on the Windows operating system and notifies consumers if their security settings put the computer at risk. The Windows XP Security Center includes the same words that appeared in the WinAntiVirus advertisement, “Security Center Help protect your PC” at the top right hand corner with a similar looking shield as well as the bulleted “Resources” list on the left. Included as **Attachment NN** is a true and correct copy of the genuine Windows XP Security Center.
183. This is confirmed by the Counterclaim in the Canadian lawsuit. Marc D’Souza states that the Business utilized, “third party trademarks or likeness to confuse consumers into misidentifying the source of the product.” See Ex. 17, Att. B, ¶ 107.
184. I performed a Google search on “W32.ZOTOB.C@mh” and also checked the databases of several leading antivirus and antispyware companies for information on this threat. In Google, there were only two hits, one in a foreign language, and the other was a complaint about an advertisement that displayed the same warning. I did not locate any information about this threat from leading software security firms.
185. I performed a Google search on “TrojanSPM/LX” and also checked the databases of several leading antivirus and antispyware companies for information on this threat. I found that leading software security firms did not have information on this threat except that it is falsely identified

as a threat by Defendants' software security products.

186. On or about November 21, 2007, I re-visited the URL located at <http://www.amaena.com/securityworm13/index.php?ax=1&ex=2&h=19>, this time using a standard FTC Internet Lab computer, running the latest version of Symantec Antivirus. The advertisement looked identical to the one I had viewed at the same URL the previous day when I was using a "clean" VMWare computer and when I had viewed this ad on or about May 11, 2007.

iii. DRIVECLEANER "SCANNERS" AND ADVERTISEMENTS

187. DriveCleaner is one of the Defendants' software security products. This is confirmed by Daniel Sundin's affidavit sworn February 19, 2007, from the Canadian lawsuit which lists *drivecleaner.com* as an IMI product. See Ex. 17, Att. G, ¶ 13 and Sundin Exhibit D. *Drivecleaner.com* is listed in TUCOWS CID response as belonging to the reseller Vantage Software, Daniel Sundin's company. Additionally, Whois history records show *drivecleaner.com* was previously registered to Innovative Marketing, Inc. in Belize. Moreover, according to the Microsoft CID, Kristy Ross placed advertisements with MyGeek on behalf of IMI for DriveCleaner. Consumer complaints list phone numbers assigned to James Reno for DriveCleaner and *drivecleaner.com* lists "Hosted by Setup a Host, Inc." in the subject information of the site's security certificate.
188. During the course of the investigation, I periodically reviewed the Spywaresucks web site for advertisements, URLs, and other information relating to the Defendants' software security products. On several occasions, links to Defendants' advertisements were posted on the

Spywaresucks web site.

189. Many of these links on the Spywaresucks web site included the domain *mediaplex.com* (“Mediaplex ads”). However, immediately upon visiting these links, I was redirected to a page on one of the Defendants’ web sites, such as *http://www.drivecleaner.com*. Included as **Attachment OO** is a true and correct copy of a list of Mediaplex ads from the Spywaresucks web site. I reviewed several of these advertisements over the course of the investigation in the FTC Internet Lab. The links to the Mediaplex ads I reviewed were *http://adfarm.mediaplex.com/ad/ck/xxxxx* where *xxxxx* was equal to a number. The site I was redirected to varied depending on the number I entered.

**a. REVIEW OF DRIVECLEANER ADVERTISEMENTS AND
“SCANNERS”**

190. On or about May 11, 2007, I used IE 7 on a standard computer in the FTC Internet Lab to visit several of the Mediaplex ads. For instance, when I entered the URL, *http://adfarm.mediaplex.com/ad/ck/49737* the browser was immediately redirected to a web page on *http://www.drivecleaner.com*. A pop-up dialogue box immediately appeared with no content visible in the background. The dialogue box read, “Windows Internet Explorer” in the top left hand corner and said,

NOTICE: Your computer has tracks of all adult sites you have visited. In most cases, you are not even aware of the files that get installed by themselves, violate your online privacy and could compromise your career and your marriage. These files leave tracks of your online behavior and even compromise your credit card’s security.

At the bottom of the dialogue box, it read “Would you like to install DriveCleaner to check your computer for free? (Recommended)” and included buttons that read, “OK” and

“CANCEL.” Included as **Attachment PP** is a true and correct copy of this pop-up dialogue box.

191. When I clicked on the button labeled, “CANCEL,” a web page loaded from *drivecleaner.com* that included a picture of woman laying in a bikini. On the right side of the page, there was a “scanner” which automatically appeared to be “scanning” my computer for “Sensitive Content.” As the “scanner” was running, IE 7's information bar (located under the address bar) read in part, “The website wants to install the following add-on: installdrivecleanerstart.cab from Drivecleaner, Inc.” After the “scanner” had finished running, a new dialogue box appeared that said Drive Cleaner had detected 953 Adult & Sensitive files even though I was using a “clean” computer. When I hit the back button on my browser, the program tried to install again.
- Included as **Attachment QQ** is a true and correct copy of this advertisement.

192. On or about November 20, 2007, I used a “clean” VMWare machine in the FTC Internet Lab to view the web site located at <http://adfarm.mediaplex.com/ad/ck/49725>. After entering in the URL, a pop-up dialogue box opened on my screen that looked identical to the one mentioned in Paragraph 190 that appeared when reviewing a different Mediaplex ad located at <http://adfarm.mediaplex.com/ad/ck/49737>. When I clicked the “X” button in the upper right corner of this pop-up dialogue box, I was redirected to another advertisement located at http://www.drivecleaner.com/freeware/index.php?p=20&a=0&j=0&pp=0&w=0&ex=0&ap=0&z=-5&link=keyin&ad=keyin_us_en_ed1&aff=r\n. Included as **Attachment RR** is a true and correct copy of this advertisement.

193. Along the top of this advertisement it read, “Security Administrator” and then “Attention! System stores temporary files on PC with explicit adult materials content. These files are

available to all users. Your private life may not be confidential. Anyone can access this information and compromise you.” The advertisement included a list of files found including 179 “Adult websites visited,” 21 “Illegal websites visited details,” 258 “Adult media files viewed details,” 93 “Cookie files” 1737 “Internet Explorer history URLs.” The ad indicated the “Privacy Level” on my computer was set to “Low.” There were boxes above this list that read, “brief information” and “hide files.” Included as part of **Attachment RR** is a true and correct copy of this part of the advertisement.

194. Next to “Adult websites visited” and “Illegal websites visited details” there were red hyperlinks that read, “details.” When I clicked on the first hyperlink next to “Adult Sites Visited,” it read, “Adult Sites Visited” and included a list that read, “<http://gayanalsex.com>, <http://analgames.com>, <http://getlaid.com>, <http://maturebitches.com>, <http://gaysdream.com>, <http://asianteens.net>, and 178 sites more.” Included as part of **Attachment RR** is a true and correct copy of this part of the advertisement.

195. I clicked on the “details” hyperlink next to “Illegal websites visited details” and it read, “Illegal Adult Sites Visited” and below this,

Attention! Visiting illegal sites and downloading its data is law prosecuted. You should immediately remove all the data dealing with illegal sites or you may have problems with the law. Learn more in “**hide files**” section.

Included as part of **Attachment RR** is a true and correct copy of this part of the advertisement.

196. On or about October 30, 2008, I used a “clean” VMWare machine in the FTC Internet Lab to search for DriveCleaner advertisements on Google. Among the results I found were two complaints from consumers who were redirected to advertisements on *drivecleaner.com*. Both

of these complaints included the link to which the consumer had been redirected.

197. When I clicked on the first link, http://drivecleaner.com/freeware/index.php?aid=swp_dc&lid=5993&affid=pp_28742684&mplx_cmp=swp_dc_common&ax=1&ed=1&ex=1, a pop-up dialogue box, identical to the one described in Paragraph 190 above which asked whether I wanted to “. . . install DriveCleaner (Recommended),” appeared. It did not matter whether I clicked, “CANCEL,” “OK” or “X,” a web page located at *drivecleaner.com* opened and immediately began “scanning” for “compromising and Internet track files.” Across the top of the page above the “scanner,” it read, “Erase all compromising evidence.” When it had finished, a new pop-up dialogue box indicated that 948 dangerous files had been found. Whether I clicked the “X” to close out of this pop-up dialogue box or the “NO” or “YES,” buttons, it would also attempt to download the program. Included as **Attachment SS** is a true and correct copy of the relevant portion of this complaint and the advertisement I saw which was created using the procedure described in Paragraph 8.

198. The second consumer complaint I found via the Google search on or about October 30, 2008, <http://www.drivecleaner.com/freeware/?p=20&a=1&j=1&pp=1&w=1&ex=1&ap=1&mpt=1157913427633&aid=mgcog4>, opened an advertisement identical to the one described in Paragraph 193 above which read “Security Administrator” across the top. When I clicked on “Hide Files” and “Download” next to “Drive Cleaner,” a pop-up dialogue box would appear indicating I had not completed the “scan” and that DriveCleaner was recommended. It did not matter whether I clicked, “CANCEL,” “OK” or “X,” to close out of this pop-up dialogue box, it would also attempt to download the program. Included as **Attachment TT** is a true and correct copy of the relevant portion of this complaint and the advertisement I saw which was

created using the procedure described in Paragraph 8.

b. MISPRESENTATIONS IN DRIVECLEANER ADVERTISEMENTS

199. I often visited multiple advertisements for Defendants' software security products on the same computer, in succession, on the same date. For example, on or about May 11, 2007, I reviewed numerous advertisements for DriveCleaner. One advertisement I reviewed located at <http://adfarm.mediaplex.com/ad/ck/49735>, indicated there were 624 "Pornographic and Sensitive" files found on the computer. It then asked "Erase them now?" with buttons labeled "YES" and "NO." A few minutes later, I visited the advertisement located at <http://adfarm.mediaplex.com/ad/ck/49737> which indicated there were 953 "Adult & Sensitive" files found. Included as **Attachment UU** are true and correct copies of both of these advertisements. Other than the number of files found, these advertisements looked identical to those attached to Daniel Sundin's Affidavit sworn February 19, 2007, and mentioned in Paragraph 46.
200. On or about November 21, 2007, using a "clean" VMWare computer, I re-visited the advertisement located at <http://adfarm.mediaplex.com/ad/ck/49725> that I had visited the previous day. Prior to visiting this web site on November 21, I checked the "History" in Internet Explorer and confirmed it did not show any prior web sites that had been visited. I also accessed the "Internet Options" for Internet Explorer via the "Tools" menu and cleared the "Cookies" and "Temporary Internet Files." I also reviewed the "Privacy" settings in Internet Explorer and confirmed it was set to "Medium."
201. I entered the URL and the same pop-up dialogue box appeared that read, "Would you like to

install DriveCleaner to check your computer for free? (Recommended).” When I clicked on the “X” in the upper right corner of this pop-up dialogue box, the same advertisement with the words “Security Administrator” described in Paragraph 193 above appeared on the screen.

202. The same number of objects in each category appeared as before and the same web sites were listed when I clicked on the “details” hyperlink next to “Adult websites visited.” I re-reviewed the “Privacy” settings in Internet Explorer and confirmed it was still set to “Medium” and not “Low” as the advertisement indicated. I also reviewed the files located in the “Temporary Internet Settings” folder. Instead of the 93 “Cookie files” listed in the advertisement, there were only 4 cookies and one was from Mediaplex and the other three were from *drivecleaner.com*. I also re-reviewed the Internet Explorer “History” and found instead of the 1737 sites listed in the advertisement, there was only *drivecleaner.com* and the “My computer” link.
203. I concluded these advertisements were false for several reasons. First, I often used “clean” VMWare machines, which did not contain adult content or malicious files, to view many of these advertisements. See Paragraph 6. Second, the advertisements, when viewed moments apart on the same “clean” machine, found different and conflicting numbers of threats. Third, each time I viewed these advertisements, no matter what type of computer I was using, or the date I visited them, these advertisements “detected” the same exact number of objects found in each category and the same adult web sites visited. Fourth, as discussed in more detail in the previous paragraph, I confirmed the representations made in the advertisements were false by reviewing the computer’s settings.

iv. OTHER ADVERTISEMENTS AND “SCANNERS”

204. In addition to the advertisements for WinAntiVirus, I reviewed several advertisements on *amaena.com* for Defendants’ software security products such as WinAntiSpyware, SystemDoctor, ErrorSafe, and ErrorProtector. These advertisements looked the same no matter which type of computer they were displayed upon.
205. In addition to the “scanners” I saw in several of the advertisements located on *amaena.com* and those I was redirected to from other sources (such as advertisements at *http://www.drivecleaner.com/freeware . . .*), I also reviewed several “scanners” by visiting the URL for the software security product directly. For example, I typed in the URL, *http://www.swiftcleaner.com*. In these instances, I did not see a dialogue box before viewing the “scanner.” As soon as I connected to the site, it would say, “Scan in Progress . . . WAIT A MINUTE” and would include a count of the number of objects found by the “scanner.” Some of the URLs I reviewed that included these types of “scanners” were *http://www.winsecureav.com*, *http://www.winspycontrol.com*, and *http://www.swiftcleaner.com*. Included as **Attachment VV** are true and correct copies of some of these “scanners.”
206. Some of the web sites I reviewed, such as *defensaantimalware.com* and *exterminadordevirus.com* were in foreign languages, but looked similar to the pages I had reviewed in English, and also included “scanners” on the homepages. Included as **Attachment WW** are true and correct copies of examples of some of these web sites I reviewed in a language other than English.

B. PURCHASES OF ADVANCEDCLEANER AT ADVANCEDCLEANER.COM

207. On or about March 12, 2008, I used a “clean” VMWare computer in the FTC Internet Lab to visit the web site located at *http://advancedcleaner.com/.cleaner/?p=1013&ida=swp_gronexx51&led=2822&afr=pp_2248501152*. This was the same link I had extracted from a consumer complaint that I had reviewed a day earlier and is described in Section IV.A(i) above.
208. The “scanner” found “Illegal porn content” on my PC and the exact same number of objects was found in the four sections below the “scanner” on the day before while using a standard FTC Internet Lab computer. This time, I selected, “Remove All” in the lower right corner of this advertisement and opened the file called “ADCFreeInstaller.exe.”
209. A box labeled, “AdvancedCleanerFree” appeared on my screen and read, “Welcome to the Installer.” I selected “Continue” and proceeded to install the free version of AdvancedCleaner.
210. When AdvancedCleaner had finished downloading, the program opened and began to “scan” my computer. When it had finished “scanning,” it read, “Scan is complete: 216 pieces of Adult Content found!” I had not visited any other web sites on the “clean” computer. The “scan” indicated there were several critical and dangerous items that had been found on my system. There were buttons on the bottom right hand corner of the AdvancedCleaner Free software that read, “Back” and “Clean Now.” There was also a button on the left and a link along the top that read, “Buy Now.” Included as **Attachment XX** are true and correct copies of printouts I made using the procedure described in Paragraph 8.
211. I clicked on the link labeled, “Clean Now” and a pop-up appeared that read, “216 Adult Content

Detected” along the top. It read, “WARNING! 216 pieces compromising content have been detected on your computer!” and then “Your PC stored 216 items that are dangerous to your reputation . . . To protect your family/career/property and get rid of these compromising contents, you need to hide them completely by means of AdvancedCleaner. For software registration, please click the ‘Register Now!’ button below.”

212. I clicked on the link in the bottom right hand corner that read, “Remind me later” and when I selected “Clean Now” again in the AdvancedCleaner Free program, a nearly identical pop-up appeared, except that it read, “216 Privacy Violations Found” along the top instead of, “216 Adult Content Detected.” I then clicked the button that read, “Register Now” and a new page opened that read, “Register NOW For Only \$39.95” and along the bottom it read, “Warning! 216 severe privacy violations, temporary and history records endangering your private life were found on your computer. Your computer has tracks of all adult sites you had visited . . . ”
213. I clicked on the button that read, “Click Here” and a page titled, “AdvancedCleaner - Payment Page” opened on the screen. This page looked similar to other “Payment Pages” I had viewed for Defendants’ software security products throughout the course of the investigation.
214. Along the bottom, there were three boxes that were pre-checked. One of the boxes read, “Check here to certify you agree to the Terms & Conditions,” the second read, “Sign me up for an upgrade to InternetAnonymizer . . . you will be billed a one-time charge of only USD 30,” and the third read, “I want to have Premium Support with dedicated support manager, remote control system & instant messaging consultant + call back service 24&7 ONLY for USD 24.95.” I unchecked the box for Internet Anonymizer but left the other two boxes checked.

215. I filled out the payment page using the name, Jessie Logan and a credit card that is not directly associated with the FTC. I provided the email address, "*jelogs@gmail.com*" and selected the button "Secure Purchase" at the bottom of the form.
216. A pop-up appeared that read, "Thank you for registering AdvancedCleaner. Now, full functional version of AdvancedCleaner will be installed [*sic*]" with a button labeled, "OK" at the bottom and a new web page appeared on the screen in the background. I selected "OK" and the pop-up disappeared.
217. Another web page opened. At the top of this page, it read, "Your computer is not safe till [*sic*] Software is downloaded and installation is completed!" Below this were two buttons, one reading, "Download Now" and another that read, "Click Here to Enter Members Area." Below this was an ad that read, "The Most Complete PC Solution" and listed the products called, "Computer Blocker" and "Password Inspector" with special prices were listed. Immediately below this advertisement was an onscreen receipt for my purchase of AdvancedCleaner.
218. The onscreen receipt for my purchase of AdvancedCleaner included five telephone numbers. The first phone number, (202) 904-2212, was listed as "24/7 Phone Support" and the second number, (800) 755-5909, was listed as "24/7 Toll-Free USA Phone Support." The final three numbers were all listed as international phone support for Canada, UK and Australia, respectively. The phone numbers (202) 904-2212, (800) 755-5909 and the number listed for Canada, (800) 889-5113, all are assigned to James Reno according to the Junction Networks CID response. See Attachment S.
219. The receipt also indicated the charge would appear as "supportsw.com 8007555909." Both

supportsw.com and this merchant identifier have previously been discussed and are associated with the Defendants. See Paragraph 58.

C. CALLS TO ADVANCEDCLEANER TOLL FREE SUPPORT LINE

220. Many consumers who called Reno's customer support telephone numbers, despite paying additional money for "24/7 premium support," experienced difficulty connecting. Consumers complained that they were on hold for long periods while a recorded voice indicated they were "x" number caller which would count down as the consumer waited on hold. Eventually, a pre-recorded message might come on that indicated they should leave a message but oftentimes an additional recording would indicate the mailbox was full. Many consumers complained that they did not hear back from customer support after leaving several messages.
221. Beginning on or about March 13, 2008, I placed a series of calls to the AdvancedCleaner 24/7 Toll-Free USA Support Line at (800) 755-5909. This telephone number is assigned to James Reno of ByteHosting according to the Junction Networks CID response. See Attachment S.
222. I recorded these conversations using audio recording software called CallSaver Pro. This software captures the telephone conversations via the computer's sound card and records the call in a .wav format onto a computer's hard drive. The software also logs the date and time of the recording, and automatically generates a file name based on that day and time. Immediately after I made the recordings, I played back each recording to confirm that the conversations had recorded properly.
223. After dialing the phone number, a recorded voice answered, "Thank you for calling Customer Support." I selected option number 1 for "Technical Support." I opted not to enter my order

number when prompted.

224. A different recorded voice then informed me that the current hold time was approximately 6 minutes and 37 seconds and that I could stay on the line to speak with a representative or I could leave a message. I stayed on the line and I very briefly heard music which was interrupted by another recorded voice that informed me I was "caller number 5 waiting to speak with a representative." It said the estimated hold time was now 10 minutes and 53 seconds, although it had been less than 7 minutes a moment before.
225. After almost eleven and a half minutes, a representative named "Tina" asked me for my order number. She pulled up my record and confirmed that I had purchased AdvancedCleaner. I told her that I had seen a "scan" that said there were "nasty, illegal sex pictures" on my computer and that I had purchased the program because I did not want my daughter to see those kinds of things. I explained that my brother had told me he thought it was a scam and I wanted to know whether these files had really been found on my computer.
226. Tina told me that a "pre-scanner" would "scan" the computer and tell me about possible threats found and then give me an option to purchase the program. She explained that the "scanner" advertisement was "just letting [me] know that that [sic] was something that could be stored on my hard drive" and she is not sure "why it shows what it shows other than what it read off the disk" and that something could be stored on my hard drive.
227. I told her that I didn't want my daughter to see the "illegal sex pictures" found by the "scanner." She asked me whether the computer was new or if there was a previous owner, "because it could be anything that's on the actual hard drive." I explained I purchased the program to have it

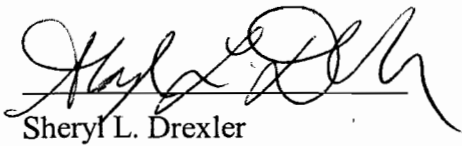
remove the files and she said maybe someone had “been on my computer that I was not aware of . . . like someone spending the night or what. But it’s—obviously, it would detect what was on there.”

228. I inquired whether my purchasing AdvancedCleaner would have removed the files from my computer and she said AdvancedCleaner “cleans up any kind of sites it’s been on and that way no one can go back in and look at the files that’s been previously viewed” and that “it cleans it, takes care of it, gets it off of there.” Tina said it “is proven to prevent you from spied on or caught with inappropriate files in your computer, keeps your drive clean, free from useless files, improving your system’s performance.”
229. I also confirmed with Tina that “after I bought it, you’re saying it got off whatever” and she said, “Right . . . yeah, you’ve already downloaded it, so it would have cleaned the files . . . it would have cleaned it up.”
230. At the end of the call, I asked Tina if I could call her back if I have other questions. She said I could call the same number I had previously called. I had previously called (800) 755-5909 but when I asked her for the support phone number, she said it was (800) 430-8969, which is another number assigned to James Reno according to the Junction Networks CID response. See Paragraph 71.

231. After speaking with Tina, I also reviewed the paychecks that were written from the ByteHosting bank account at US Bank that were received in response to the Commission's CID to US Bank. There were payroll checks written to a "Tina Hughes" from ByteHosting's account. See Paragraph 96.

I declare under penalty of perjury that the foregoing statement is true and correct.

Executed on November 26, 2008.


Sheryl L. Drexler

DREXLER DECLARATION - ATTACHMENT A					
Domain Name	Whois Date	Registrant Name	Company Name	Registrant Contact Information	Source
advancedcleaner.com	4/28/2008	AdvancedCleaner Inc.		402 S Medical Dr Bountiful, UT 84010 USA hostmaster@advancedcleaner.com 801-295-9844	Whois Record
amaena.com	12/10/2005	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
billingnow.com	7/10/2003	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
burnads.com	7/10/2003	Ines Hadden		48, boulevard de Port Royal Paris, FRANCE 75005 burnads_c@yahoo.com 164233375	Whois Record
buysmarter.com	9/6/2003	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
bytecenter.com	11/24/2008	ByteCenter Web Services, LLC	ByteHosting Internet Services, LLC (Technical Contact)	3864 McMann Road STE A Cincinnati, OH 45245 USA dnsadmin@bytehosting.com 8668946192	Whois Record
bytehosting.com	12/22/2004	James Reno	ByteHosting Internet Services	PO BOX 820 & PO Box 104 Amelia, OH 45102 USA admin@bytehosting.com	Whois History
	11/24/2008		ByteHosting Internet Services, LLC	3864 McMann Road STE A Cincinnati, OH 45245 USA dnsadmin@bytehosting.com 8668946192	Whois Record
computershield.com	7/29/2003	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History

Domain Name	Whois Date	Registrant Name	Company Name	Registrant Contact Information	Source
dataconfidentiality.com	12/22/2007		Hostmaster, WebHosts Inc (Technical Contact)	1876 Hutson Street Belize City, BELIZE no_name_inc@yahoo.com 555-123-1234	Whois History
	11/24/2008	Contactprivacy.com		96 Mowat Ave Toronto, Ontario CANADA M6K 3M1 dataconfidentiality@contactprivacy.com +1.4165385457	Whois Record
drivecleaner.com	9/4/2004	Innovative Marketing, Inc.		1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
	4/9/2008	Tone, Ricardo Da	DriveCleaner, Inc.	32 Maxwell Road #03-07 Whitehouse Singapore, NA 069115 +65 6715 8018 no_name_inc@yahoo.com	Whois Record
drivecleaner.net	5/24/2006	Hostmaster, Vantage	Vantage Software	2711 Centerville Rd. Wilmington, DE 19808 USA daniel.sundin@engelholm.se 555-123-1234	Whois History
errorprotector.com	3/15/2006	Innovative Marketing, Inc.		1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
errorsafe.com	8/8/2005	Panzotto, Jardim	ErrorSafe, Inc.	1878 [sic] Hutson Street Belize City, BELIZE info@errorsafe.com +1.7865130214	Whois History
forceup.com	4/29/2008	admin, hostmaster	forceup	34 Cumberland Street Toronto, CANADA M5R 1A3 mydomains0@yahoo.com 1.4165551122	Whois History
	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record

Domain Name	Whois Date	Registrant Name	Company Name	Registrant Contact Information	Source
globedat.com	8/11/2005	Setuphost	Smith, Ann	PO Box 2122 Toronto, ONT, CANADA K9J 7Y4 dnsadmin@setuphost.net 1.8007555909	Whois History
innovativemarketing.com	12/15/2002	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History TUCOWS CID
	4/10/2006	Hostmaster, Vantage	Vantage Software, Inc.	2711 Centerville Rd. Wilmington, DE 19808 USA hostmaster@vantagesoftware.com 555-123-1234	TUCOWS CID
	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record
malwarecrush.com	4/9/2008	Domain Admin	PrivacyProtect.org	PO Box 97 Moergesteel, NETHERLANDS 5066 contact@privacyprotect.org 4536946676	Whois Record
multimediafixer.com	9/4/2004	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record

Domain Name	Whois Date	Registrant Name	Company Name	Registrant Contact Information	Source
pcsupercharger.com	9/4/2004	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Huison Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
	11/24/2008	Contactprivacy.com		96 Mowat Ave Toronto, Ontario CANADA M6K 3M1 pcsupercharger.com@ contactprivacy.com +1.4165385457	Whois Record
popupguard.com	12/20/2003	Hostmaster, Vantage	Vantage Software, Inc.	2711 Centerville Rd. Wilmington, DE 19808 USA daniel.sundin@engelholm.se 555-123-1234	Whois History
	4/30/2008	Hostmaster, Vantage	Vantage Software Inc, LTD	Green Dragon House 64-70 High Street hostmaster@popupguard.com +44-20-7900-2196	Whois Record
revenueerresponse.com	12/7/2005	admin, hostmaster	revenueerresponse	1876 Huison Street Belize City, BELIZE hostmaster@revenueerresponse.com +380.979390944	Whois History
setupahost.net	1/21/2005		Setup A Host	P.O Box 2122 Peterborough, Ontario, CANADA 7Y4 dnsadmin@setupahost.net +1.9052483003	Whois History
	1/18/2004	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Huison Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
stopguard.com	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record
	8/2/2007	Hostmaster, SupportSW	Support SW	C/ Sant Feliu, 19 Palma de Mallorca, ES [SPAIN] 07012 hostmaster@supportsw.com 34 971 49 52 13	Whois History

Domain Name	Whois Date	Registrant Name	Company Name	Registrant Contact Information	Source
sysprotect.com	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record
systemdoctor.com	9/4/2004	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
vantagesoftware.com	5/24/2004	Hostmaster, Vantage	Vantage Software Inc. Ltd.	Green Dragon House 64-70 High Street Croydon, Surrey, UK CR09XN hostmaster@vantagesoftware.com daniel.sundin@engelholm.se +44-20-7900-2196	Whois History
	4/17/2006	Hostmaster, Vantage	Vantage Software Inc.	2711 Centerville Rd. Wilmington, DE 19808 USA hostmaster@vantagesoftware.com 555-123-1234	TUCOWS CID
	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record
virussw.com	11/24/2008	Administration, DNS	SYNERGY SOFTWARE B.V.	Dokweg 27 B Ijmuiden, CA USA 1976 dnsadmin@virussw.com +31 251 416555	Whois Record
winadblocker.com	3/31/2005	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com daniel@pmmci.com 555-123-1234	Whois History
	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record

Domain Name	Whois Date	Registrant Name	Company Name	Registrant Contact Information	Source
winantispay.com	9/4/2004	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record
winantispyware.com	9/3/2005	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
	4/15/2008	WinAntiSpyware		P.O. Box 3 Kiev, UKRAINE 04114 hostmaster@winantispyware.com +(380) 97 939 09 44	Whois Record
winantivirus.com	1/22/2004	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
	2/2/2004	Hostmaster, WinAntiVirus	WinAntiVirus	P.O. Box 37 Kiev, UKRAINE 01103 hostmaster@winantivirus.com +380 44 496 04 59	Whois History
	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record

Domain Name	Whois Date	Registrant Name	Company Name	Registrant Contact Information	Source
winantiviruspro.com	12/22/2004	Administrator, DNS	WinAntiVirus	P.O. Box 3 Kiev, UKRAINE 04114 dnadmin@winantiviruspro.com +(380) 97 939 09 44	Whois History
	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record
wincontentfilter.com	5/9/2006	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record
windrivecleaner.com	5/9/2006	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record
winfixer.com	6/1/2005	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
	9/17/2005	Hostmaster, WinFixer	WinFixer	P.O. Box 3 Kiev, UKRAINE 04114 hostmaster@winfixer.com +(380) 97 939 09 44	Whois History TUCOWS CID
winsecureav.com	4/15/2008	S. Conant, Garland	LocusSoftware Inc.	Trg revolucije 19 Brusnice, SLOVENIA S18321 no_name_inc@yahoo.com +1.416555112251234	Whois Record

Domain Name	Whois Date	Registrant Name	Company Name	Registrant Contact Information	Source
winsoftware.com	5/18/2004	Hostmaster, Innovative	Innovative Marketing, Inc.	1876 Hutson Street Belize City, BELIZE hostmaster@innovativemarketing.com 555-123-1234	Whois History
	11/14/2005	Hostmaster, WinSoftware	WinSoftware, Inc.	P.O. Box 3 Kiev, UKRAINE 04114 hostmaster@winsoftware.com +(380) 97 939 09 44	Whois History
	11/24/2008	Anonymizer, Whois	Whois Anonymizer	Rua da Paz 1471 Sao Paulo, NA CEP, BRAZIL 04713-001 hostmaster@whoisanonymizer.com +1.6468451873	Whois Record
winspycontrol.com	4/19/2008	S. Conant, Garland	LocusSoftware Inc.	Trg revolucije 19 Brusnice, SLOVENIA SI8321 no_name_inc@yahoo.com +1.416555112251234	Whois Record

CIVIL INVESTIGATIVE DEMAND
File No. 9923259

winfixer.com
vantagesoftware.com
innovativemarketing.com

III. Document Specifications

A. Payment information

Reseller has this information. Contact info attached.

*** Please note that Reseller appears to also be owner of domain in some instances.

B. Correspondence

We have provided the registration records for each domain, as they were when they were transferred into our system, and as they currently are. Any other correspondence would be with the reseller.

C. Additional Domains

We have attached a list of domains wherein the registrant is the same.



CIVIL INVESTIGATIVE DEMAND

1. TO

Tucows, Inc.
Attn: Sandra Cooper, Compliance Officer
96 Mowat Avenue
Toronto, Ontario Canada M6K 3M1

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

☐ You are required to appear and testify.

LOCATION OF HEARING

YOUR APPEARANCE WILL BE BEFORE

DATE AND TIME OF HEARING OR DEPOSITION

*Do Not
Disclose to
Respondent*

☒ You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

☒ You are required to answer the interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

April 4, 2006

3. SUBJECT OF INVESTIGATION

See attached resolution.

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN

C. Steven Baker/Theresa J. Bresnahan
Federal Trade Commission, Midwest Region
55 E. Monroe St., #1860
Chicago, IL 60603

5. COMMISSION COUNSEL

Jason K. Bowler
Federal Trade Commission, Midwest Region
(312) 960-5607
312-960-5600 (fax)

DATE ISSUED

MARCH 22, 2006

COMMISSIONER'S SIGNATURE

William E. Kovach

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from

Form of Certificate of Compliance*

I/We do certify that all of the documents required by the attached Civil Investigative Demand which are in the possession, custody, control, or knowledge of the person to whom the demand is directed have been submitted to a custodian named herein.

If a document responsive to this has not been submitted, the objection to its submission and the reasons for the objection have been stated.

Signature

Title

J. Cooper
Compliance officer

Sworn to before me this day

17 April 2006.
Brenda Tazare
Notary Public

*In the event that more than one person is responsible for complying with this demand, the certificate shall identify the documents for which each certifying individual was responsible. In place of a sworn statement, the above certificate of compliance may be supported by an unsworn declaration as provided for by 28 U.S.C. § 1746.

Current Server Time: Mon Apr 10 17:02:54 2006

UTC: Mon Apr 10 21:02:54 2006

[Main menu](#)

Reg System Orders

Total: 2

<u>ID</u>	<u>Reseller</u>	<u>Domain</u>	<u>Language</u>	<u>Type</u>	<u>Status</u>	<u>Email</u>	<u>Affiliate ID</u>	<u>Order Date</u>	<u>Period</u>
33659073	vantage	winfixer.com		Renewal	Completed	hostmaster@innovativemarketing.com		2005-07-23 00:01:47	1
12636737	vantage	winfixer.com		Transfer	Completed	hostmaster@innovativemarketing.com		2004-01-26 22:53:00	1

registration
record

Live System
osrs2

Current Server Time: 17/Apr/2006 14:04:14 EDT
UTC: Mon Apr 17 18:04:14 2006

[Back to Main Menu](#)

Domain Order Edit Form

original contact info

Domain Information

Registration Type: Transfer

Domain Name: winfixer.com

Status: Completed

Profile: redeempresents.com

Affiliate ID:

Transfer Information:

Transfer Status: Completed

Transfer Domain Locked: No

Are contact changes required?: No

Owner Request Date: 10:53 pm Jan 26, 2004

Owner Confirmation Date: 11:13 pm Jan 26, 2004

Registry Request Date: 11:48 pm Jan 26, 2004

[View Order Notes\(1\)](#)

Contact Information

First Name: Innovative

Last Name: Hostmaster

Organization Name: Innovative Marketing, Inc.

Street Address: 1876 Hutson Street

(eg: Suite #245):

Address 3:

City: Belize City

State: NA

2 Letter Country Code: BZ

Postal Code:

Phone Number: 555-123-1234

Fax Number: 555-123-1234

Email: hostmaster@innovativemarketing.com

Admin Information

First Name: Innovative

Last Name: Hostmaster

Organization Name: Innovative Marketing, Inc.

Street Address: 1876 Hutson Street

(eg: Suite #245):

Address 3:

ATTACHMENT B

City: Belize City
State: NA
2 Letter Country Code: BZ
Postal Code:
Phone Number: 555-123-1234
Fax Number: 555-123-1234
Email: hostmaster@innovativemarketing.com

Billing Information

First Name: Innovative
Last Name: Hostmaster
Organization Name: Innovative Marketing, Inc.
Street Address: 1876 Hutson Street
(eg: Suite #245):
Address 3:

City: Belize City
State: NA
2 Letter Country Code: BZ
Postal Code:
Phone Number: 555-123-1234
Fax Number: 555-123-1234
Email: hostmaster@innovativemarketing.com

Technical Contact Information

First Name: Innovative Marketing, Inc.
Last Name: Hostmaster
Organization Name: Innovative Marketing, Inc.
Street Address: 1876 Hutson Street
(eg: Suite #245):
Address 3:

City: Belize
State: NA
2 Letter Country Code: BZ
Postal Code: 12345
Phone Number: +1.5551231234
Fax Number: +1.5551231234
Email: hostmaster@innovativemarketing.com

DNS Information

Primary DNS Hostname: ns1.iad1.nssrv.com
Secondary DNS Hostname: ns2.iad1.nssrv.com
Third DNS Hostname:
Fourth DNS Hostname:

ATTACHMENT B

Fifth DNS Hostname:

Sixth DNS Hostname:

ATTACHMENT B

Live System

osrs2

Current Server Time: Mon Apr 10 17:04:05 2006

UTC: Mon Apr 10 21:04:05 2006

[Main menu](#)**winfixer.com***current info*[Manage Domain as Registrant](#)[Modify Domain](#)[View Domain Notes \(12\)](#)[View All Domain Notes \(12\)/Add Internal Notes](#)**Reseller: vantage****Expiration Date: 2006-08-20 00:26:14****Registrant Username: vantage****Organization Information****First Name: WinFixer****Last Name: Hostmaster****Organization Name: WinFixer****Street Address: P.O. Box 3****City: Kiev****State: NA****2 Letter ISO Country Code: UA****Postal Code: 04114****Phone: +(380) 97 939 09 44****Fax:****Email: hostmaster@winfixer.com****Admin Information****First Name: WinFixer****Last Name: Hostmaster****Organization Name: WinFixer****Street Address: P.O. Box 3****City: Kiev****State: NA****2 Letter ISO Country Code: UA****Postal Code: 04114****Phone: +(380) 97 939 09 44****Fax:**

ATTACHMENT B

Email: hostmaster@winfixer.com

Billing Information

First Name: WinFixer

Last Name: Hostmaster

Organization Name: WinFixer

Street Address: P.O. Box 3

City: Kiev

State: NA

2 Letter ISO Country Code: UA

Postal Code: 04114

Phone: +(380) 97 939 09 44

Fax:

Email: hostmaster@winfixer.com

Technical Contact Information

First Name: WinFixer

Last Name: Hostmaster

Organization Name: WinFixer

Street Address: P.O. Box 3

City: Kiev

State: NA

2 Letter ISO Country Code: UA

Postal Code: 04114

Phone: +(380) 97 939 09 44

Fax:

Email: hostmaster@winfixer.com

DNS Information

FQDN

IP

ns8.nscache.net

ns9.nscache.net

ATTACHMENT B

Reseller Information – winfixer.com

[\[top menu\]](#)

Tech Contact	
First Name	Innovative Marketing, Inc.
Last Name	Hostmaster
Title	
Organization Name	Innovative Marketing, Inc.
Street Address	1876 Hutson Street
[eg: Suite #245]	
Address 3	
City	Belize
State	NA
2 Letter Country Code	Belize
Postal Code	12345
Phone Number	+1.5551231234 [eg. 416-555-1122 x333]
Fax Number	+1.5551231234 [eg. 416-555-1122 x333]
Email	hostmaster@innovativemarketing.com

Current Server Time: Mon Apr 10 17:06:57 2006
UTC: Mon Apr 10 21:06:57 2006

[Main menu](#)

Reg System Orders

registration record

Total: 5

ID	Reseller	Domain	Language	Type	Status	Email	Affiliate ID	Order Date	Per
31872883	vantage	vantagesoftware.com		Renewal	Completed	hostmaster@vantagesoftware.com		2005-06-07 00:05:38	1
15103181	vantage	vantagesoftware.com		Renewal	Completed	hostmaster@vantagesoftware.com		2004-06-03 23:58:28	1
9950768	vantage	vantagesoftware.com		Renewal	Completed	hostmaster@vantagesoftware.com		2003-06-03 23:39:20	1
5417233	vantage	vantagesoftware.com		Transfer	Completed	hostmaster@vantagesoftware.com		2002-02-07 11:53:13	1
5165225	vantage	vantagesoftware.com		Transfer	Cancelled	hostmaster@vantagesoftware.com		2002-01-14 01:44:06	1

Live System
osrs2

Current Server Time: 17/Apr/2006 14:07:34 EDT
UTC: Mon Apr 17 18:07:34 2006

[Back to Main Menu](#)

Domain Order Edit Form

original info

Domain Information

Registration Type: Transfer

Domain Name: vantagesoftware.com

Status: Completed

Profile: redeempresents.com

Affiliate ID:

Transfer Information:

Transfer Status: Completed

Transfer Domain Locked: No

Are contact changes required?: No

Owner Request Date: 11:53 am Feb 7, 2002

Owner Confirmation Date: 11:56 am Feb 7, 2002

Registry Request Date: 12:03 pm Feb 7, 2002

[View Order Notes\(1\)](#)

Contact Information

First Name: Vantage

Last Name: Hostmaster

Organization Name: Vantage Software, Inc.

Street Address: 2711 Centerville Rd.

(eg: Suite #245):

Address 3:

City: Wilmington

State: DE

2 Letter Country Code: US

Postal Code: 19808

Phone Number: 555-123-1234

Fax Number: 555-123-1234

Email: hostmaster@vantagesoftware.com

Admin Information

First Name: Vantage

Last Name: Hostmaster

Organization Name: Vantage Software, Inc.

Street Address: 2711 Centerville Rd.

(eg: Suite #245):

Address 3:

ATTACHMENT B

City: Wilmington

State: DE

2 Letter Country Code: US

Postal Code: 19808

Phone Number: 555-123-1234

Fax Number: 555-123-1234

Email: hostmaster@vantagesoftware.com

Billing Information

First Name: Vantage

Last Name: Hostmaster

Organization Name: Vantage Software, Inc.

Street Address: 2711 Centerville Rd.

(eg: Suite #245):

Address 3:

City: Wilmington

State: DE

2 Letter Country Code: US

Postal Code: 19808

Phone Number: 555-123-1234

Fax Number: 555-123-1234

Email: hostmaster@vantagesoftware.com

Technical Contact Information

First Name: Vantage

Last Name: Hostmaster

Organization Name: Vantage Software, Inc.

Street Address: 2711 Centerville Rd.

(eg: Suite #245):

Address 3:

City: Wilmington

State: DE

2 Letter Country Code: US

Postal Code: 19808

Phone Number: 555-123-1234

Fax Number: 555-123-1234

Email: daniel.sundin@engelholm.se

DNS Information

Primary DNS Hostname: ns1.integrationsoft.com

Secondary DNS Hostname: ns2.integrationsoft.com

Third DNS Hostname:

Fourth DNS Hostname:

ATTACHMENT B

Fifth DNS Hostname:

Sixth DNS Hostname:

ATTACHMENT B

Live System
osrs2

Current Server Time: Mon Apr 17 14:06:58 2006
UTC: Mon Apr 17 18:06:58 2006

[Main menu](#)

current info

vantagesoftware.com

[Manage Domain as Registrant](#)

[Modify Domain](#)

[View Domain Notes \(18\)](#)

[View All Domain Notes \(18\)/Add Internal Notes](#)

Reseller: vantage

Expiration Date: 2006-07-01 06:51:21

Registrant Username: vantage

Organization Information

First Name: Vantage

Last Name: Hostmaster

Organization Name: Vantage Software

**Street Address: Casilla 87-10, Suc. El Golf
Las Condes**

City: Santiago de Chile

State: NA

2 Letter ISO Country Code: CL

Postal Code: 7550000

Phone: +56 2 6298397

Fax: +56 2 6298397

Email: hostmaster@vantagesoftware.com

Admin Information

First Name: Vantage

Last Name: Hostmaster

Organization Name: Vantage Software

**Street Address: Casilla 87-10, Suc. El Golf
Las Condes**

City: Santiago de Chile

State: NA

2 Letter ISO Country Code: CL

Postal Code: 7550000

Phone: +56 2 6298397

Fax: +56 2 6298397

ATTACHMENT B

Page 99

Email: hostmaster@vantagesoftware.com

Billing Information

First Name: Vantage

Last Name: Hostmaster

Organization Name: Vantage Software

Street Address: Casilla 87-10, Suc. El Golf
Las Condes

City: Santiago de Chile

State: NA

2 Letter ISO Country Code: CL

Postal Code: 7550000

Phone: +56 2 6298397

Fax: +56 2 6298397

Email: hostmaster@vantagesoftware.com

Technical Contact Information

First Name: Vantage

Last Name: Hostmaster

Organization Name: Vantage Software

Street Address: Casilla 87-10, Suc. El Golf
Las Condes

City: Santiago de Chile

State: NA

2 Letter ISO Country Code: CL

Postal Code: 7550000

Phone: +56 2 6298397

Fax: +56 2 6298397

Email: hostmaster@vantagesoftware.com

DNS Information


FQDN

IP

ns8.nscache.net

ns9.nscache.net

Reseller Information – **vantagesoftware.com**[\[top menu\]](#)

Tech Contact	
First Name	Innovative Marketing, Inc.
Last Name	Hostmaster
Title	
Organization Name	Innovative Marketing, Inc.
Street Address	1876 Hutson Street
[eg: Suite #245]	
Address 3	
City	Belize
State	NA
2 Letter Country Code	Belize 
Postal Code	12345
Phone Number	+1.5551231234 [eg. 416-555-1122 x333]
Fax Number	+1.5551231234 [eg. 416-555-1122 x333]
Email	hostmaster@innovativemarketing.com

Main menu

Reg System Orders

registration record

Total: 4

<u>ID</u>	<u>Reseller</u>	<u>Domain</u>	<u>Language</u>	<u>Type</u>	<u>Status</u>	<u>Email</u>	<u>Affiliate ID</u>	<u>Order I</u>
47072636	vantage	innovativemarketing.com		Renewal	Completed	hostmaster@innovativemarketing.com		2006-04-0 00:40:49
29602090	vantage	innovativemarketing.com		Renewal	Completed	hostmaster@innovativemarketing.com		2005-04-0 00:14:12
6943345	vantage	innovativemarketing.com		<u>Transfer</u>	Completed	hostmaster@vantagesoftware.com		2002-07-1 20:07:11
6837254	vantage	innovativemarketing.com		<u>Transfer</u>	Cancelled	hostmaster@vantagesoftware.com		2002-07-0 07:34:00

Live System
osrs2

Current Server Time: 10/Apr/2006 17:10:20 EDT
UTC: Mon Apr 10 21:10:20 2006

[Back to Main Menu](#)

original info

Domain Order Edit Form

Domain Information

Registration Type: Transfer

Domain Name: innovativemarketing.com

Status: Completed

Profile: redeempresents.com

Affiliate ID:

Transfer Information:

Transfer Status: Completed

Transfer Domain Locked: No

Are contact changes required?: No

Owner Request Date: 8:07 pm Jul 12, 2002

Owner Confirmation Date: 8:40 pm Jul 12, 2002

Registry Request Date: 9:02 pm Jul 12, 2002

[View Order Notes\(2\)](#)

Contact Information

First Name: Vantage

Last Name: Hostmaster

Organization Name: Vantage Software, Inc.

Street Address: 2711 Centerville Rd.

(eg: Suite #245):

Address 3:

City: Wilmington

State: DE

2 Letter Country Code: US

Postal Code: 19808

Phone Number: 555-123-1234

Fax Number: 555-123-1234

Email: hostmaster@vantagesoftware.com

Admin Information

First Name: Vantage

Last Name: Hostmaster

Organization Name: Vantage Software, Inc.

Street Address: 2711 Centerville Rd.

(eg: Suite #245):

Address 3:

ATTACHMENT B

City: Wilmington
State: DE
2 Letter Country Code: US
Postal Code: 19808
Phone Number: 555-123-1234
Fax Number: 555-123-1234
Email: hostmaster@vantagesoftware.com

Billing Information

First Name: Vantage
Last Name: Hostmaster
Organization Name: Vantage Software, Inc.
Street Address: 2711 Centerville Rd.
(eg: Suite #245):
Address 3:

City: Wilmington
State: DE
2 Letter Country Code: US
Postal Code: 19808
Phone Number: 555-123-1234
Fax Number: 555-123-1234
Email: hostmaster@vantagesoftware.com

Technical Contact Information

First Name: Vantage
Last Name: Hostmaster
Organization Name: Vantage Software, Inc.
Street Address: 2711 Centerville Rd.
(eg: Suite #245): Apt 1123
Address 3:

City: Wilmington
State: DE
2 Letter Country Code: US
Postal Code: 19808
Phone Number: 555-123-1234
Fax Number: 555-123-1234
Email: hostmaster@vantagesoftware.com

ATTACHMENT B

Live System
osrs2

Current Server Time: Mon Apr 10 17:10:40 2006
UTC: Mon Apr 10 21:10:40 2006

[Main menu](#)

Current info

innovativemarketing.com

[Manage Domain as Registrant](#)

[Modify Domain](#)

[View Domain Notes \(15\)](#)

[View All Domain Notes \(15\)/Add Internal Notes](#)

Reseller: vantage

Expiration Date: 2007-05-05 00:00:00

Registrant Username: vantage

Organization Information

First Name: Innovative

Last Name: Hostmaster

Organization Name: Innovative Marketing, Inc.

Street Address: 1876 Hutson Street

City: Belize City

State: NA

2 Letter ISO Country Code: BZ

Postal Code:

Phone: 555-123-1234

Fax: 555-123-1234

Email: hostmaster@innovativemarketing.com

Admin Information

First Name: Innovative

Last Name: Hostmaster

Organization Name: Innovative Marketing, Inc.

Street Address: 1876 Hutson Street

City: Belize City

State: NA

2 Letter ISO Country Code: BZ

Postal Code:

Phone: 555-123-1234

Fax: 555-123-1234

ATTACHMENT B

Page 105

Email: hostmaster@innovativemarketing.com

Billing Information

First Name: Innovative

Last Name: Hostmaster

Organization Name: Innovative Marketing, Inc.

Street Address: 1876 Hutson Street

City: Belize City

State: NA

2 Letter ISO Country Code: BZ

Postal Code:

Phone: 555-123-1234

Fax: 555-123-1234

Email: hostmaster@innovativemarketing.com

Technical Contact Information

First Name: Innovative

Last Name: Hostmaster

Organization Name: Innovative Marketing, Inc.

Street Address: 1876 Hutson Street

City: Belize City

State: NA

2 Letter ISO Country Code: BZ

Postal Code:

Phone: 555-123-1234

Fax: 555-123-1234

Email: hostmaster@innovativemarketing.com

DNS Information

FQDN


IP

ns8.nscache.net

ns9.nscache.net

ATTACHMENT B

Reseller Information – **innovativemarketing.com**[\[top menu\]](#)

Tech Contact	
First Name	Innovative Marketing, Inc.
Last Name	Hostmaster
Title	
Organization Name	Innovative Marketing, Inc.
Street Address	1876 Hutson Street
[eg: Suite #245]	
Address 3	
City	Belize
State	NA
2 Letter Country Code	Belize 
Postal Code	12345
Phone Number	+1.5551231234 [eg. 416-555-1122 x333]
Fax Number	+1.5551231234 [eg. 416-555-1122 x333]
Email	hostmaster@innovativemarketing.com

[Sign Out](#)

Current Folder: **None**

[Compose](#) [Addresses](#) [Folders](#) [Options](#) [Search](#) [Help](#)

[Tucows Home](#)

Viewing a text attachment - [View message](#)

[Download this as a file](#)

123digit.com
123digits.com
18gay.com
accuratelotto.com
adconversion.com
adconvert.com
adpatrol.com
adservant.com
adultlots.com
adultmatchline.com
adultmatchservice.com

NAME

advertisingcontrol.com
adwareprofit.com
allvirgin.com
alternativedate.com
alternativesluts.com
altmatchservice.com
alumnis.com
amaena.com
amateurhoney.com
amateurhoneys.com
amateurhousing.com

NAME

amateurlots.com
amateurprofit.com
amateursasia.com
amateurtwins.com
americancreampie.com
americancreampies.com
ampleteens.com
analkatie.com
analkelly.com
analleah.com
analnewcomers.com
analpies.com
analreamers.com
analtooral.com
analtovaginal.com
annasfriends.com
annsfriends.com
antivirii.com
antivirus-comparison.com
anyclicks.com
anywherespy.com
arisnetworks.com

NAME

arsesluts.com
asiamatchservice.com
asianboobies.com
asiandistrict.com
asianmatchservice.com
asianperversion.com
asianperversions.com
asiansexmatch.com
asiantitties.com
asscreampies.com
assdrippers.com

NAME

asseatinggirls.com
assfuckedmilf.com
assfuckedmilfs.com
assfuckedmom.com
assfuckedmoms.com
assfuckedtwinks.com
assfucksurprise.com
assspankin.com
auctionofferings.com
babypokers.com
backupcontrol.com
balloonfuck.com
balloonfucking.com
barelyfemale.com
bbwsexmatch.com
bdsmasia.com
bdsmlesbians.com
bdsmmatchservice.com
bestofonlinesearch.com
bestsearchnet.com
betbonus.com
bigboobamateurs.com

NAME

bigboobsbigbutts.com
bigboobsroundbutts.com
bigbootyamateurs.com
biggerblackerbetter.com
billcomplete.com
billingcomplete.com
billinginfo.com
billingkey.com
billingnow.com
billingticket.com
billnow.com

NAME

billticket.com
bitdownload.com
bitdownloader.com
bizarrecash.com
bizarremom.com

bizarremoms.com
bizarreprofit.com
bizarrestories.com
bizarreteens.com
blackcockblondeass.com
blackcockswhiteasses.com

NAME

blackcockwhitemoms.com
blackcockwhitewife.com
blackcockwhitewives.com
blackdistrict.com
bleedingsluts.com
blingfinder.com
blingmatch.com
blondesfuckingblacks.com
bloodsluts.com
bondageasia.com
bondagedates.com
bondageonly.com
bondagesingles.com
bookmyfares.com
boysdrinkingpiss.com
boystats.com
brazilianmovieparadise.com
brokerprofit.com
brutalmistress.com
brutalmistresses.com
brutalplay.com
bukakeasia.com

NAME

bukkakedreams.com
bukakefantasies.com
bukaketv.com
burbonstreetsluts.com
bustyporno.com
bustyxxx.com
buy-smarter.com
cafebi.com
cafepiss.com
cafestud.com
cafestuds.com

NAME

camprofits.com
camsprofit.com
candidconnections.com
candidsmut.com
cartoonsmut.com
cartoonstuds.com
cashflowguides.com
cashfordriving.com
cashguides.com
casinoacehigh.com
casinoaceking.com

NAME

casinoaceshigh.com
casinopresidential.com
casualflings.com
celebprofit.com
celebritieshardcore.com
celebrityl8.com
celebrityteenies.com
celebrityundressed.com
celebsleaze.com
cellphoneprofit.com
chatguardian.com
cheerleaderaudition.com
chestyteens.com
chicksdrunk.com
chicksflashing.com
chicksgonenuts.com
chokeoncock.com
chokeoncocks.com
chokesoncock.com
christiandistrict.com
christianhalo.com
christianmatchservice.com

NAME

clearanceink.com
clickwwwsearch.com
clubslave.com
clubslaves.com
cockenhancer.com
cockslapping.com
coedfuckbuddies.com
coedsasia.com
coedsexbuddies.com
coedsjapan.com
collegefuckbuddies.com

NAME

collegesexdating.com
communityconcept.com
completebill.com
completebilling.com
computeranywhere.com
computercleaner.com
computerrecovery.com
computershield.com
computersupercharger.com
contentpatrol.com
contentprotector.com

NAME

contentreview.com
contentreviewer.com
contentshield.com
copymovies.com
crashprotector.com

creampieambush.com
creampiecocktail.com
creampiecocktails.com
creampietrick.com
creditprofit.com
creditrecord.com
creditrecords.com
creditrenovation.com
creditrepairs.com
creditsecretsguide.com
creditsecretsguides.com
cryingcunts.com
cryingsluts.com
cumdrippingasses.com
cumshotorgies.com
cumswappingboys.com
cursordistrict.com

NAME

curvyasians.com
cuteboytoys.com
cutrateink.com
daddiesboys.com
daddiesdarling.com
daddiesdarlings.com
daddiesslut.com
daddiessluts.com
daddyfuckingson.com
daddyfucksson.com
dadfuckingson.com

NAME

dadfucksson.com
datepass.com
datingcams.com
datingprofit.com
debtprofit.com
deepthroatxxx.com
desk2ads.com
deskadult.com
deskamateur.com
deskamateurs.com
deskanimals.com

NAME

deskanime.com
deskaquarium.com
deskasians.com
deskaction.com
deskuctions.com
deskbdsm.com
deskbet.com
deskbetting.com
deskbikinis.com
deskbondage.com
deskbooty.com
deskbuy.com

deskcams.com
deskcars.com
deskcartoons.com
deskcats.com
deskceleb.com
deskcelebrities.com
deskcelebs.com
deskcell.com
deskcheerleaders.com
deskcheerlearer.com

NAME

deskcircus.com
deskdancers.com
deskdate.com
deskdates.com
deskdating.com
deskdogs.com
deskdownload.com
deskdownloads.com
deskfacials.com
deskfun.com
deskgreeting.com

NAME

deskgreetings.com
deskhardcore.com
desk hentai.com
deskhumor.com
deskhumour.com
deskjenna.com
deskjerkoff.com
deskjungle.com
deskkid.com
deskkids.com
desklivecam.com

NAME

desklivecams.com
desklivefeeds.com
desk liveshows.com
deskmatch.com
deskmobiles.com
deskmodel.com
deskmodels.com
deskmp3.com
desk nude.com
desk nurse.com
desk nurses.com
deskorgies.com
deskorgy.com
deskpersonal.com
deskpersonals.com
deskplumpers.com
deskporn.com
deskprofit.com
desksecretaries.com

desksecretary.com
deskshemale.com
deskshemales.com

NAME

desksportscars.com
deskspy.com
desksupermodel.com
desksupermodels.com
desktoons.com
desktransexuals.com
desktranssexuals.com
deskvideo.com
deskvideos.com
deskwomen.com
deskxxx.com

NAME

deskzoo.com
dialerprofit.com
dietingfast.com
dietprofit.com
dietquickly.com
discreetfling.com
discreetflings.com
discreetgirlfriend.com
discreetmatch.com
discreetsexlife.com
discreetwives.com

NAME

discretegirlfriend.com
discretematch.com
discretensexlife.com
discretewives.com
diskprotector.com
divorceinstruction.com
divorceinstructions.com
dormroomlovers.com
dormroommatch.com
dormsmut.com
dormvoyeurs.com
doublepenetrationsluts.com
download-centrals.com
downloadcontrol.com
downloadmp3snow.com
doyourneighbor.com
doyourneighbors.com
doyourneighbour.com
doyourneighbours.com
dpsluts.com
drive-cleaner.com
drivecleaner.com

NAME

drivefixer.com

driveforpay.com
driveprotection.com
driveprotector.com
drownedsluts.com
drowningsluts.com
drugprofit.com
drugssource.com
drugswizard.com
drunkgals.com
dungeonslaves.com

NAME

easycheaters.com
ebonysexmatch.com
ebonytranssexual.com
economyink.com
emailmedia.com
emailprotector.com
emailsspy.com
enemahotties.com
enemasluts.com
entranceticket.com
erectionstore.com

NAME

erotichousing.com
errorprotect.com
errorprotector.com
escorhotties.com
evidenceeraserpro.com
extremepublicpissing.com
ezcheaters.com
facefuckedher.com
facefuckingher.com
facesitsluts.com
facesittingsluts.com
fantasytwink.com
fantasytwinks.com
farmhotties.com
farmsmut.com
fartinglesbians.com
fartingmovies.com
fartmovies.com
fartsluts.com
fastercomputer.com
fetishhousing.com
fetishmatchfinder.com

NAME

fetishmatchservice.com
fetishsexmatch.com
filefixer.com
fileprotector.com
fistedmen.com
fistfuckedboys.com
fistfuckedher.com
fistfuckedmen.com

fistingaction.com
fistinghotties.com
fistsluts.com

NAME

flashersluts.com
footservant.com
footservants.com
footservitude.com
freeadultmatch.com
freecreditrecords.com
freedebtelimination.com
freematchservice.com
freepornticket.com
freewwwsite.com
freewwwsites.com

NAME

frenchmatchservice.com
friendsflirting.com
fuckbuddycam.com
fuckbuddycams.com
fuckbuddymatch.com
fuckedherface.com
fuckedinthecity.com
fuckedroughly.com
fuckingbareback.com
furryguys.com
gagginggirls.com
gaggingsex.com
gagging sluts.com
gagging surprise.com
gagsurprise.com
gamblingprofit.com
gangbangambush.com
gangbangaudition.com
gangeduponher.com
ganginguponher.com
ganguponher.com
ganguponme.com

NAME

gapingsluts.com
gayaccesspass.com
gaycumswappers.com
gaydebutantes.com
gaydebutants.com
gaydesire.com
gaydistrict.com
gayflings.com
gaygiganticcocks.com
gaylots.com
gaymatchfinder.com

NAME

gaymatchservice.com

gaypissdrinking.com
gaysexbuddies.com
gaysexmatch.com
gayticket.com
gayuniformed.com
genericbrowser.com
genericscanner.com
generictoolbar.com
genielotto.com
germanmatchservice.com

NAME

getfreecar.com
getgovernmentgrants.com
getgovtgrants.com
getjavagames.com
giftcardforfree.com
giftcardsforfree.com
giftprofit.com
giganticcocksex.com
giganticdicksex.com
giganticmellons.com
giganticmelons.com
girlfucksboy.com
girlfucksboys.com
girlsucksboys.com
girlslickingass.com
girlyguys.com
gloryholesurprise.com
goapeshit.com
gooeyfaces.com
gorgeousfeet.com
gothporno.com
gotprofit.com

NAME

great-bizdeals.com
greetingsspy.com
hairlessbeaver.com
hairyhoney.com
handstied.com
hardgangbangs.com
haveamazingsex.com
hbill.com
hentaihotties.com
herbalharden.com
herbalprofit.com

NAME

hersexteacher.com
heshestories.com
hiddenstats.com
hinduporno.com
hisexteacher.com
hollywood-female.com
hookedphonics.com
hornycamsluts.com

hornylivesluts.com
hotcams.com
hotcumswappers.com

NAME

hotenemas.com
hotgaycam.com
hotliveamateurs.com
hotliveasians.com
hotliveblacks.com
hotlivegay.com
hotlivegirls.com
hotlivelatinas.com
hotlivemature.com
hotlivenetwork.com
hotlivenetworks.com
hotlivenubians.com
hotliveplump.com
hotliveshemales.com
hotlifestuds.com
hotlivetgirls.com
hotlivetwinks.com
hotpetite.com
hotravers.com
hugeorgies.com
hammerfuck.com
hammerfucking.com

NAME

hammerhump.com
hammerhunter.com
hammersex.com
hungjocks.com
imagefixer.com
immediatefunds.com
incestualaffairs.com
incestualhardcore.com
incestualmovies.com
incestualsex.com
incestualstories.com

NAME

incestualteens.com
incestualtoons.com
incestualvideos.com
indianmatchservice.com
inkclearance.com
inkprofit.com
innovativemarketing.com
innovativeness.com
innovativeventures.net
installationcontrol.com
installcontrol.com

NAME

installprofit.com

instantmp3download.com
internetantispay.com
internetblocker.com
internetrefunds.com
internetspy.com
interracialhoneys.com
interracialpenetration.com
interracialtrannies.com
intrudertrace.com
intrudertracer.com
intrusiontrace.com
intrusiontracer.com
investorsgenie.com
invisiblestats.com
italianmatchservice.com
janasplace.com
japanesecreampies.com
japanesenipples.com
japanesepies.com
japaneseteenies.com
japanesetwinks.com

NAME

javagamespro.com
jenswallows.com
jewdistrict.com
jewishdistrict.com
jewishmatchservice.com
jizzbuckets.com
jizzfarters.com
jizzshooters.com
justpornstars.com
justteensmovies.com
justwantsex.com

NAME

katiesplayhouse.com
kazaagolddownload.com
kazaaupgrade.com
kazamp3download.com
keywordcpv.com
kinkdates.com
kinkfriends.com
kinkier.com
knockedherup.com
kpremium.com
lactatinghotties.com

NAME

latexgals.com
latexhotties.com
latinadistrict.com
latinamatchservice.com
latinasmut.com
latinmatchservice.com
latinomatchservice.com
leadprofit.com

leechspy.com
leggoddess.com
leggoddesses.com
lesbianassfuckers.com
lesbianasslovers.com
lesbianandominance.com
lesbianperversions.com
lesbianrimming.com
lesbiansexmatch.com
lesbianslickingass.com
lesbianspankings.com
lifefuckingsucks.com
lightplumpers.com
lilgirlbigcock.com

NAME

liquidharden.com
liquidvirility.com
listmanagerpro.com
littleboobies.com
littlegirlbigcock.com
littleleah.com
littletops.com
livefeedprofit.com
liveinvestigator.com
liveshowprofit.com
localfuckbuddies.com

NAME

localsexbuddies.com
localsexbuddy.com
mailconfirmation.com
maleamateurs.com
malehollywood.com
malevoyeurism.com
massiveorgies.com
masterkarmasutra.com
matchprofit.com
matchservice.com
maturelots.com

NAME

maturepussies.com
maturesmut.com
mcafeereview.com
mediafixer.com
membersspot.com
membersticket.com
menfuckboys.com
menfucksboys.com
mensanswers.com
messyhoes.com
messyhotties.com
mildplumpers.com
milfchaser.com
milffuckbuddies.com
milffuckbuddy.com

miniaturebrowser.com
miniaturescanner.com
miniaturetoolbar.com
miraclepenis.com
mistresspain.com
mommiesslut.com
mommiessluts.com

NAME

mommyfuckers.com
momsassfuck.com
momsassfucked.com
momsassfucking.com
morpheusmp3download.com
mortgagequickly.com
mp3downloadclub.com
mp3snow.com
multimediafixer.com
mylittlepussy.com
naivevirgins.com

NAME

nakedpublicly.com
nastyeve.com
nastyinsertion.com
nastyinsertions.com
naughtybrunettes.com
naughtypiercings.com
naughtyredheads.com
naughtyswingers.com
naughtykatie.com
naughtykelly.com
netgirlfriends.com

NAME

netsupercharger.com
netturbopro.com
networkprotector.com
networksnoop.com
networksnooper.com
neverbeenfucked.com
newsoftoday.com
nextdoorasians.com
nextdoorhoney.com
nextdoorhoneys.com
nfriends.com
nikkisplayhouse.com
nipponamateur.com
nipponamateurs.com
nipponbukkake.com
nipponscat.com
nipponschoolgirls.com
nipponsluts.com
nocostcar.com
nortoncomparison.com
nubianhotties.com
nudityoutdoors.com

NAME

nylonhotties.com
okfuckthat.com
oldfuckingyoung.com
onestoponlineshop.net
onlineshield.com
onlybondage.com
optimizedlotto.com
optimizelotto.com
orgasmenhancer.com
orientalperversion.com
orientalperversions.com

NAME

orientalshemale.com
orientalsin.com
orientaltwink.com
pantyhosehoneys.com
pantyhotties.com
pantytramps.com
pcsupercharger.com
pcturbopro.com
peeasians.com
peeingguys.com
peeingjapanese.com

NAME

peeingtwinks.com
penisenhancer.com
periodsluts.com
personalspass.com
personalsprofit.com
perverteddates.com
pervertedmatch.com
petfantasy.com
petsuncensored.com
pillprofit.com
pillsprofit.com
pissasians.com
pissdaughter.com
pissdaughters.com
pissdreams.com
pissdrinkingboys.com
pissduo.com
pissduos.com
pissfantasies.com
pissingjapanese.com
pissrain.com
pissrains.com

NAME

pissreceptacles.com
playfulamy.com
playfulnikki.com
pleasecuminme.com

plumpchicks.com
ponysluts.com
poopingsluts.com
popupnukerpro.com
pornaccesspass.com
pornhousing.com
pornohousing.com

NAME

pornolots.com
pornstarxxx.com
pornticket.com
pregnantsmut.com
premiumcallgirls.com
prescriptionsources.com
prettyorpity.com
privacyprotector.com
privacyutilities.com
privacyutils.com
privatefling.com

NAME

privateflings.com
profitchat.com
profitlottery.com
profitprograms.com
profitremote.com
profitreward.com
profitstats.com
programleech.com
proxyprotector.net
publicgoldenshowers.com
publicnudebeach.com
publicnudebeaches.com
publicpissdrinking.com
publicpissplay.com
pukesluts.com
pukingsluts.com
pureboys.com
qualitysoftware.com
quick-picks.com
quickcleanup.com
ranchhotties.com
rapedlesbians.com

NAME

rapedream.com
rapedreams.com
rbill.com
rbilling.com
realityprofit.com
redeempresents.com
refundsfromhome.com
reliablestats.com
remotescout.com
remotespy.net
removeemail.com

NAME

reunionprofit.com
reunionsonline.com
review-software.com
rewardprofit.com
rewardsprofit.com
ringtonegold.com
roughlyfucked.com
salesticket.com
saraswallows.com
scatasia.com
scatasians.com

NAME

scatcinema.com
scatdominance.com
scatdream.com
scatdreams.com
scatfantasies.com
scatfantasy.com
search42.com
searchfindsearch.com
secretadorer.com
secretaryhotties.com
secretfling.com
secretflings.com
secretgirlfriend.com
secretlovelife.com
securewipe.com
securityalert.com
semenfarters.com
seniormatchservice.com
setupaserver.com
sexbuddies.com
sexdatingcam.com
sexdatingcams.com

NAME

sexdesire.com
sexdiscreet.com
sexenhancer.com
sexlots.com
sexprofit.com
sexualwives.com
sexykatya.com
sexylena.com
sexyover40.com
shanghaiboys.com
shavedjapan.com

NAME

shechokesoncock.com
shejerksit.com
shemalehoneys.com
sheswallows.net

shitfantasies.com
shitflicks.com
shitlesbians.com
sleepingsluts.com
slimeyfacials.com
sloppyloads.com
slutmakeover.com

NAME

slutsdrunk.com
slutsfighting.com
slutssquirt.com
slutssquirting.com
slutswrestle.com
sluttyescorts.com
sluttyravers.com
sluttysmokers.com
smileydistrict.com
smotheredsluts.com
smutflicks.com
snowballsluts.com
socialcommunities.com
sodomizedboys.com
sodomizedgirls.com
sodomizedsluts.com
softplumpers.com
softwareleech.com
softwareoutfit.com
softwareprofit.com
spamprofit.com
spamprotector.com

NAME

spankedtwinks.com
spankinass.com
spankthatass.com
speeddrive.com
spermgobblers.com
spermtasters.com
spitgirls.com
spitlesbians.com
spittinglesbians.com
sportsbookprofit.com
springbreakexposed.com

NAME

spyremote.com
squirtinghotties.com
statsclient.com
statscompanion.com
statstrend.com
statstrends.com
stattrends.com
stickyloads.com
stockpops.com
stocksprofit.com
stopguard.com

NAME

straponcoeds.com
 straponfucked.com
 strippedstars.com
 studalley.com
 studfantasies.com
 submissivetwinks.com
 sugardaddydate.com
 sugardaddydating.com
 surf-patrol.com
 surfpatrol.com
 svcdomain.com
 swallowmypiss.com
 sweetjen.com
 symantecreview.com
 systemdoctor.com
 systemshield.com
 tattoobitches.com
 teamsluts.com
 teenagebeastiality.com
 teenagebestiality.com
 teenagepee.com
 teenbizarre.com

NAME

teenhousing.com
 teenlots.com
 teenperversion.com
 teenperversions.com
 teenplumpers.com
 teenshavers.com
 tgirlfucksgirl.com
 tgirlfucksgirls.com
 tgirlsfuckgirls.com
 tgirlsurprise.com
 thickasians.com

NAME

thickcumshots.com
 thickfacials.com
 throatfuckedher.com
 throatfuckingher.com
 ticketprofit.com
 ticketsprofit.com
 ticklesluts.com
 ticklingsluts.com
 tightamateurs.com
 tinyboobies.com
 tinygirlbigcock.com

NAME

toonsmut.com
 torturedlesbians.com
 torturegirls.com
 torturelesbians.com

tortureslaves.com
totallynasty.com
totallynaughty.com
totallyshemale.com
traceintruder.com
traceintruders.com
traceintrusion.com
tramplesluts.com
tramplingsluts.com
transexualhotties.com
transsexualhotties.com
twinkasia.com
twinkhotties.com
twinkspeeing.com
ultranews.com
unaturalinsertions.com
uncensoredpets.com
undressedcelebrities.com

NAME

undressedstars.com
uniformedgay.com
uniformedguys.com
uninstallcontrol.com
unlimitedgreetings.com
unlimitedlyrics.com
unnaturalinsertions.com
unusualinsertion.com
unusualinsertions.com
upskirthoneys.com
upskirthotties.com

NAME

usbukkake.com
vantagehelp.com
vantagescanner.com
vantagesoftware.com
videonewcomer.com
videonewcomers.com
videotryout.com
videotryouts.com
violentplay.com
vipfares.com
virginbutt.com

NAME

virus-guard.com
virusguard.com
virussoftwarereview.com
visaprofit.com
voluptuousxxx.com
vomitsluts.com
wagersdirect.com
wantprofit.com
webamateur.com
webinvestigator.com
webmasterdistrict.com

webvoyeurs.com
whitefucksblack.com
wideopenasses.com
wildnudebeach.com
wildnudebeaches.com
winadblocker.com
winadkiller.com
winanny.com
winantiad.com
winantiads.com
winantiadware.com

NAME

winantifraud.com
winantipopup.com
winantipopups.com
winantispam.com
winantispy.com
winantispyware.com
winantivirus.com
winantiviruspro.com
winanywhere.com
winbonuspack.com
winbonuspak.com

NAME

wincleandrive.com
wincontentfilter.com
wincookie.com
windatarecovery.com
windefender.com
windowsadblocker.com
windowsantispam.com
windowsantispy.com
windowsanywhere.com
windowspopupstopper.com
windowsrecovery.com

NAME

windowsrestore.com
windowssupercharger.com
windrivecleaner.com
windrivesafe.com
wineasyrecovery.com
wineliminator.com
winemailfilter.com
winfilesafe.com
winfirewall.com
winfixer.com
winfixers.com

NAME

winidentityguard.com
wininternetsecurity.com
wininternetspy.com
wininvestigator.com

winnanny.com
winpluspack.com
winpluspak.com
winpopupguard.com
winpopupkiller.com
winpopupstopper.com
winprivacyguard.com

NAME

winprivacyshield.com
winproductions.com
winremotely.com
winrestore.com
winscanner.com
winshield.com
winsitter.com
winsoftware.com
winspamblocker.com
winspamkiller.com
winsupercharger.com

NAME

winsurfpatrol.com
winsurveillance.com
wintrace.com
wivesatplay.com
workhome-center.com
wramble.com
xxxhousing.com
xxxlots.com
youdumbfucks.com
youngasia.com
youngfuckingold.com

NAME

youngfuckold.com
youngnplump.com
youngplump.com
youngplumpers.com
zaov.com
zoav.com

Transformix
IT Management

Spyware Detail

Winfixer E

Date Published:

Tuesday, May 20, 2008

Threat Assessment

Overall Risk: **High**

Privacy: **Medium**

Productivity: **Medium**

System Integrity: **Medium**

Characteristics

Category : Trojan

Also known as: Win32/Winfixer.E

Immediate Protection Info

DAT Release	Product	DAT Version
Original	eTrust PestPatrol v5	05 21 2008
	CA Antispyware v9	05 21 2008
	eTrust PestPatrol v8	05 21 2008
Latest	eTrust PestPatrol v5	10 23 2008
	CA Antispyware v9	10 27 2008
	eTrust PestPatrol v8	10 23 2008

Tools [Scan for Spyware](#) [Submit a Sample](#)

- [Description](#)
- [Origins](#)
- [Operation](#)
- [Removal](#)
- [Research](#)

Attachment C

Description

Category

Trojan: Any program with a hidden intent. Trojans are one of the leading causes of breaking into machines. If you pull down a program from a chat room, new group, or even from unsolicited e-mail, then the program is likely trojaned with some subversive purpose. The word Trojan can be used as a verb: To trojan a program is to add subversive functionality to an existing program. For example, a trojaned login program might be programmed to accept a certain password for any user's account that the hacker can use to log back into the system at any time. Rootkits often contain a suite of such trojaned programs.

[Back to top](#)

Origins

Date of Origin

date of origin: May, 2008

[Back to top](#)

Operation

- Winfixer E: at least Winfixer EKB

[Back to top](#)

Removal

Detections:

true

Executable Files:

Attachment C

Files:

20080519-trojans.zip
printsrv32.exe
printsrv32.exe

File Analysis

- Winfixer E

[Back to top](#)

Research

- [AllTheWeb](#)
- [AltaVista](#)
- [AOL Search](#)
- [Ask Jeeves](#)
- [Google](#)
- [HotBot](#)
- [Lycos](#)
- [LookSmart](#)
- [MSN](#)
- [Yahoo!](#)

Computer Associates eTrust PestPatrol

[Back to top](#)

Copyright © 2008 CA

Transforming
IT Management

Spyware Detail

WinAntiVirus Pro 2006

Date Published:

Thursday, June 1, 2006

Threat AssessmentOverall Risk: **High**Privacy: **Medium**Productivity: **Medium**System Integrity: **Medium****Characteristics****Category :** Trojan**Also known as:** winantivirus pro [Webroot]**Immediate Protection Info**

DAT Release	Product	DAT Version
Original	CA Antispyware v9	06 02 2006
	eTrust PestPatrol v5	06 02 2006
	eTrust PestPatrol v4	06 02 2006
	eTrust PestPatrol v8	06 02 2006
Latest	CA Antispyware v9	10 27 2008
	eTrust PestPatrol v5	10 23 2008
	eTrust PestPatrol v4	12 29 2006
	eTrust PestPatrol v8	10 23 2008

Tools [Scan for Spyware](#) [Submit a Sample](#)

- [Description](#)
- [Origins](#)
- [Operation](#)

- [Removal](#)
- [Research](#)

Description

Vendor Description

WinSoftware is a world-class business services company focused on delivering first-class security solutions to a wide range of clients. Our software is mostly designed to help individuals, small businesses and educational organizations to secure their computers from different threats coming from all sides and growing in number and complexity. We provide a complementary range of products and services that enable every customer to choose the product that suits him/her best. Our solutions include virus protection, content and advertising filtering, firewall solutions, optimization software and more.

Category

Trojan: Any program with a hidden intent. Trojans are one of the leading causes of breaking into machines. If you pull down a program from a chat room, new group, or even from unsolicited e-mail, then the program is likely trojaned with some subversive purpose. The word Trojan can be used as a verb: To trojan a program is to add subversive functionality to an existing program. For example, a trojaned login program might be programmed to accept a certain password for any user's account that the hacker can use to log back into the system at any time. Rootkits often contain a suite of such trojaned programs.

Reasons For Retention

This program provides, displays fake alerts, and downloads other programs onto user's machine without permission.

[Back to top](#)

Origins

Author

URL

url: <http://winantivirus.com/>

Date of Origin

date of origin: June, 2006

[Back to top](#)

Operation

- WinAntiVirus Pro 2006: at least WinAntiVirus Pro 2006KB

[Back to top](#)

Removal**Detections:**

true

Executable Files:

true

Autorun References:

HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\runonce
fat.exe
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run
winantiviruspro2006

DLL Files:

%program_files%\winantivirus pro 2006\winpgi.dll
%program_files%\winantivirus pro 2006\wav6com.dll
%program_files%\winantivirus pro 2006\sqlite3.dll
%program_files%\winantivirus pro 2006\sporder.dll
%program_files%\winantivirus pro 2006\rulsrv.dll
%program_files%\winantivirus pro 2006\plugins\update\uadaily.dll
%program_files%\winantivirus pro 2006\rpt.dll
%program_files%\winantivirus pro 2006\plugins\update\ua27308.dll
%program_files%\winantivirus pro 2006\plugins\update\ua27307.dll

Registry Items:

HKEY_CLASSES_ROOT\antiviruscom.avofficeprotect
HKEY_CLASSES_ROOT\antiviruscom.avofficeprotect.1
HKEY_CLASSES_ROOT\antiviruscom.avofficeprotect.1\clsid
HKEY_CLASSES_ROOT\antiviruscom.avofficeprotect\clsid
HKEY_CLASSES_ROOT\appid\{367a86a5-d048-4785-86be-4e2706aafdd9}
HKEY_CLASSES_ROOT\appid\winpgi.dll appid
HKEY_CLASSES_ROOT\avexplorer.shellexextension
HKEY_CLASSES_ROOT\avexplorer.shellexextension.2
HKEY_CLASSES_ROOT\avexplorer.shellexextension.2\clsid

Files:

wapchk{5c092e82-a2b0-442b-bc0b-b84bda5ffbd1}.dll
wav6com.dll
winantivirus pro 2006 manual.lnk
winantivirus pro 2006.lnk
winantiviruspro2006freeinstall.exe
%profile%\local settings\temp\~wa6psetup.exe
%profile%\local settings\temp\icdl.tmp\uwa6p_0001_n91m1807netinstaller.exe
%profile%\local settings\temp\icdl.tmp\uwa6p_0001_n91m1807netinstaller.inf
winantiviruspro2006freeinstall_de.exe

Directories:

%profile%\application data\winantivirus pro 2006
%program_files%\common files\companion wizard
%program_files%\common files\winantivirus pro 2006
%program_files%\winantivirus pro 2006
%program_files%\winantivirus pro 2006\awbase
%program_files%\winantivirus pro 2006\awbase\database
%program_files%\winantivirus pro 2006\download
%program_files%\winantivirus pro 2006\img
%program_files%\winantivirus pro 2006\pgbase

File Analysis

- WinAntiVirus Pro 2006

[Back to top](#)

Research

- [AllTheWeb](#)
- [AltaVista](#)
- [AOL Search](#)
- [Ask Jeeves](#)
- [Google](#)
- [HotBot](#)
- [Lycos](#)
- [LookSmart](#)
- [MSN](#)
- [Yahoo!](#)

Computer Associates eTrust PestPatrol

[Back to top](#)

Copyright © 2008 CA

Main Index

HOME SMALL
USERS BUSINESS ENTERPRISES PARTNERS
SECURITY ABOUT
CENTER F-
SECURE



Select language

[日本語](#) | [簡/繁体中文](#) | [繁體中文\(香港\)](#) | [繁體中文\(臺灣\)](#)

Main Index » Security Centre » Descriptions

F-Secure Spyware Information Pages: Winfixer

[\[Summary\]](#) | [\[Detailed Description\]](#)

Name: **Winfixer**

Alias: Winantispware, WinAntiSpy, ErrorSafe, WinAntiVirus, WinAntiVirusPro, Systemdoctor, Downloader.Win32.Winfixer

Type: **Rogue**Category: **Spyware**Platform: **W32**

Summary

Winfixer is an application that is installed by drive-by downloads and ActiveX installations. The program starts automatically at boot-up and presents to remove problems it has found.

Detailed Description


Winfixer, made by Winsoftware, is an application to fix problems in Windows. It is mainly installed by drive-by downloads and ActiveX installations. Winfixer doesn't offer the trial version on their website, it can only be purchased from there.

The software runs automatically and starts up each time the operating system starts. Scan is issued automatically to maximize visualisation to users of false errors and employs scare tactics with questions to the user asking if they want to keep the errors or purchase the full version of the software.

Winsoftware seems to be affiliated with another company called Vantage Software who, despite claims to be headquartered in Croydon, England, ErrorSafe and WinAntiSpy are two other companies who have re-branded Winfixer and offer it for sale on their sites. Winfixer can also be found in

Please also see the description for Zlob for additional details and a removal tool.

F-Secure Corporation

- [Copyright & Privacy](#) |
- [Contact Us](#) |
- 

Security Guide

F-Secure World Map

Security Alerts

Virus Statistics

Malware Removal Tools

Malware Code Glossary

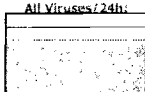
Submit Malware Sample

Select local site

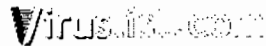
Global Sites



Global Alert Level:
- Medium -



1.1 Anti-Malware engine per Hour
5. Download 1 Trial Versions

[All Threats](#)[Viruses](#)[Hackers](#)[Spam](#)[Whole site](#) [Viruses](#)[Go](#)[Viruslist.com Search](#)[Home](#) / [Search](#)

Search

[All site search](#)[Virus search](#)[Search](#)☐ Check this box to only search viruses which have a description☐ Check this box to search for Kaspersky Lab names only (no aliases included in search)

Phrase to find: "winfixer"

Found: 129

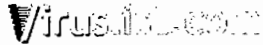
1. [Trojan.Win32.Small.ju](#) aka spr/dldr winfixer i.101
No description available
2. [not-a-virus:Downloader.Win32.WinFixer.a](#)
No description available
3. [not-a-virus:Downloader.Win32.WinFixer.aa](#)
No description available
4. [not-a-virus:Downloader.Win32.WinFixer.ab](#)
No description available
5. [not-a-virus:Downloader.Win32.WinFixer.ac](#)
No description available
6. [not-a-virus:Downloader.Win32.WinFixer.ad](#)
No description available
7. [not-a-virus:Downloader.Win32.WinFixer.ae](#)
No description available
8. [not-a-virus:Downloader.Win32.WinFixer.af](#)
No description available
9. [not-a-virus:Downloader.Win32.WinFixer.ag](#)
No description available
10. [not-a-virus:Downloader.Win32.WinFixer.ah](#)
No description available

[Next Page >>](#)

The Virus Search only searches the virus database, which contains Kaspersky Lab malware names and all available aliases for each name. It does not search the entire site.

The Site Search searches the entire site, including the Virus Encyclopedia. It only searches for whole words, and not for strings, as the Virus Search does. Therefore a search conducted with Virus Search will give different results from those shown for a Site Search.

Attachment C

[All Threats](#)[Viruses](#)[Hackers](#)[Spam](#)[Whole site](#) [Viruses](#)[Go](#)[Viruslist.com Search](#)[Home](#) / [Search](#)

Search

[All site search](#)[Virus search](#)[Search](#)☐ Check this box to only search viruses which have a description☐ Check this box to search for Kaspersky Lab names only (no aliases included in search)

Phrase to find: "advancedcleaner"

Found: 5

1. **not-a-virus:Downloader.Win32.AdvancedCleaner.a**
No description available
2. **not-a-virus:Downloader.Win32.AdvancedCleaner.b**
No description available
3. **not-a-virus:Downloader.Win32.AdvancedCleaner.c**
No description available
4. **not-a-virus:FraudTool.Win32.AdvancedCleaner.a**
No description available
5. **not-a-virus:FraudTool.Win32.AdvancedCleaner.b**
No description available

The Virus Search only searches the virus database, which contains Kaspersky Lab malware names and all available aliases for each name. It does not search the entire site.

The Site Search searches the entire site, including the Virus Encyclopedia. It only searches for whole words, and not for strings, as the Virus Search does. Therefore a search conducted with Virus Search will give different results from those shown for a Site Search.

Attachment C



Winfixer

Type	Program
SubType	Win32
Discovery Date	09/01/2005
Length	Varies
Minimum DAT	4572 (09/01/2005)
Updated DAT	5416 (10/27/2008)
Minimum Engine	5.1.00
Description Added	09/01/2005
Description Modified	12/01/2005 5:11 PM (PT)

Risk Assessment

Corporate User	N/A
Home User	N/A

Overview

This is a Potentially Unwanted Program (PUP) detection. It is not a virus or trojan. PUPs are any piece of software which a reasonably security-or privacy-minded computer user may want to be informed of.

Characteristics

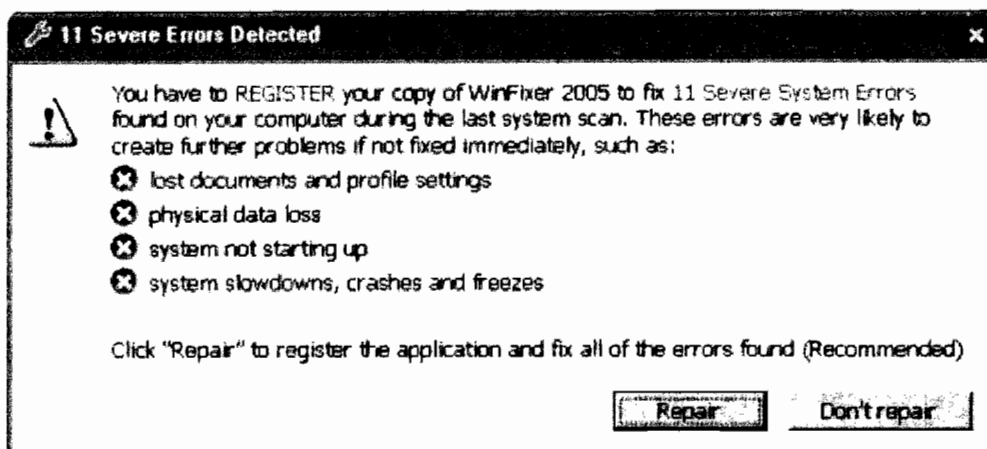
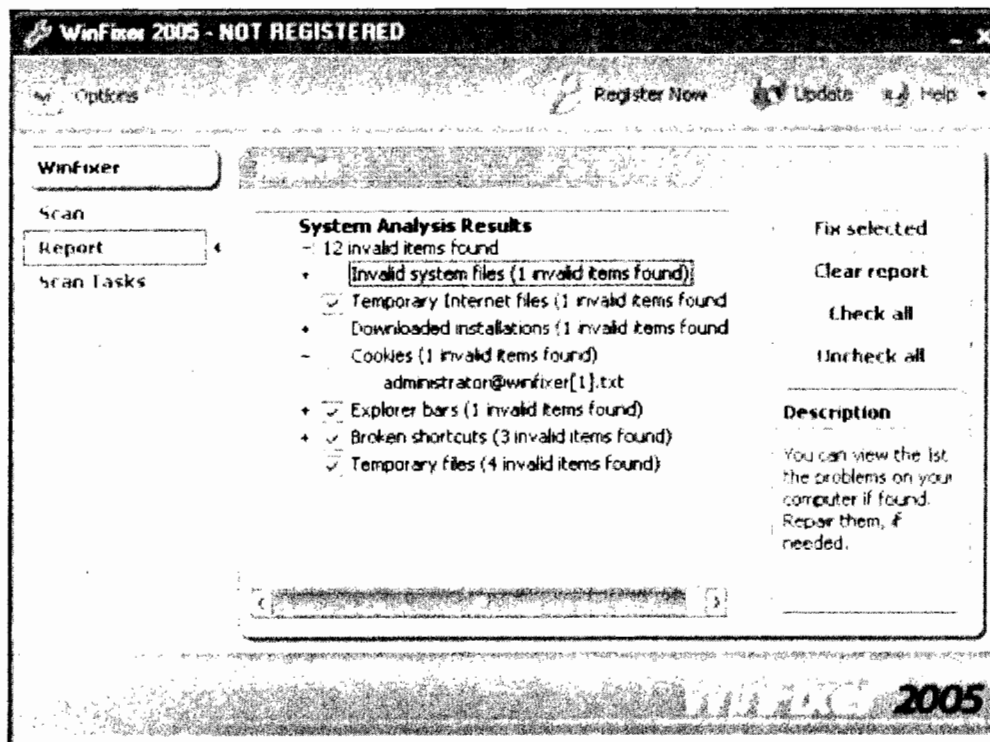
McAfee(R) AVERT recognizes that this program may have legitimate uses in contexts where an authorized administrator has knowingly installed this application. If you agreed to a license agreement for this, or another bundled application, you may have legal obligations with regard to removing this software, or using the host application without this software. Please contact the software vendor for further information.

See <http://vil.nai.com/vil/DATReadme.asp> for a list of Program detections added to the DATs.

See <http://vil.nai.com/vil/pups/configuration.htm> for information about how to enable, disable, and exclude detection of legitimately installed programs.

Distribution

This is not a virus or a trojan. It is detected as a "potentially unwanted program." It purports to be an system repair/maintenance application, but requires paid registration before any issues found can be fixed. Many of the "invalid" items found appear suspect. For example, a cookie from the winfixer.com domain was detected, along with several shortcuts that were pointing to valid existing targets. Although some detected items may be legitimate, the fact that clearly benign items are cited as problems is questionable. The primary function of the free version appears to be to alarm the user into paying for registration, at least partially based on false or erroneous detections.



Other incarnations of this software exist with the same model and similar web presences, coming from the same IP address range. For example, ErrorSafe (www.errorsafe.com, 66.244.254.63) claims to protect a user from system errors, corrupt data, and crashes.

Winfixer has been known to get installed silently through code exploiting Microsoft Internet Explorer vulnerabilities.

Privacy

No privacy policy is displayed during installation. However, a policy can be accessed online: <http://www.winfixer.com/privacy.html>.

System Changes

General defaults for typical path variables (although they may be different, they usually are not):

%WinDir% = \WINDOWS (Windows 9x/ME/XP), \WINNT (Windows NT/2000)

%SystemDir% = \WINDOWS\SYSTEM32 (Windows 9x/ME/XP), \WINNT\SYSTEM32 (Windows NT/2000)

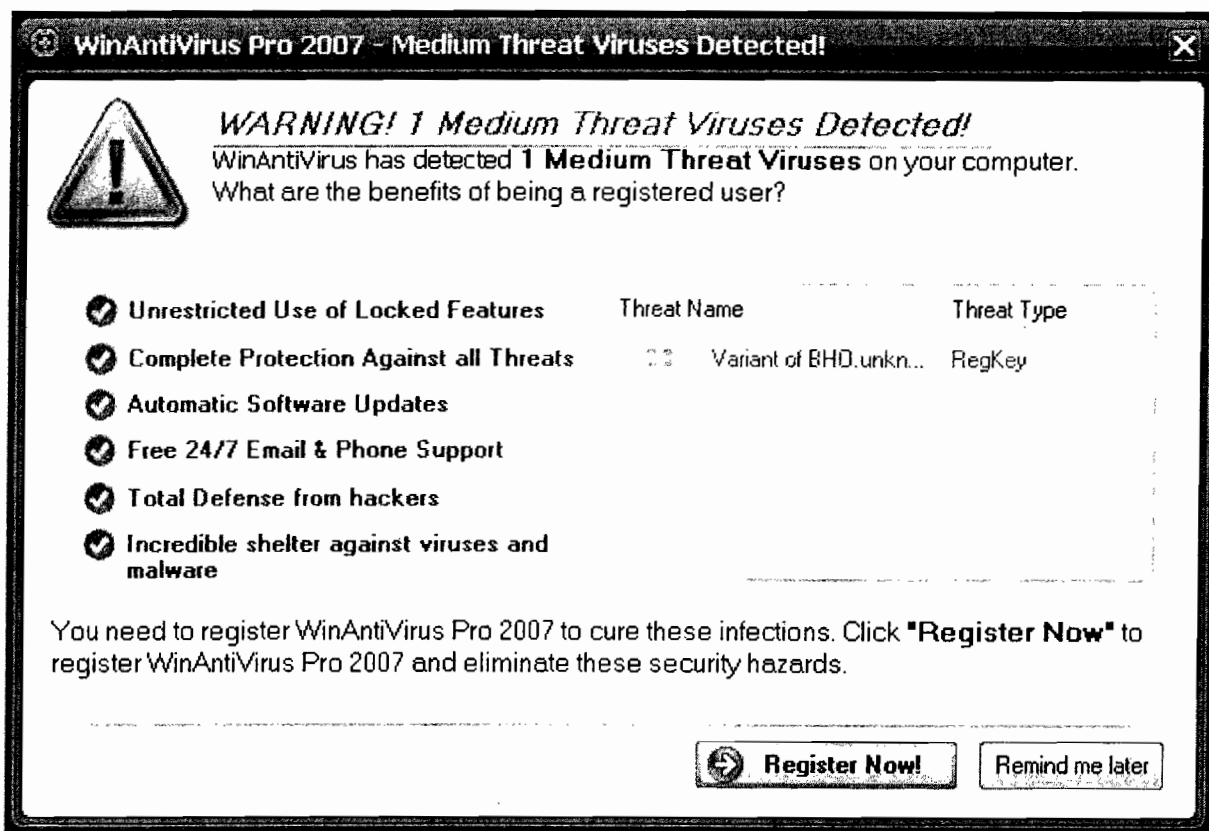
%ProgramFiles% = \Program Files

"" - Denotes files that, though installed along with the software, are by themselves innocent and not included in detection.

Source: <http://www.microsoft.com/security/portal/Entry.aspx?Name=Program%3aWin32%2fWinSoftware.WinAntiVirus>

Technical Information

Program: Win32/WinSoftware is a program that displays warnings or malware detections, in order to prompt users to purchase WinAntiVirus. Below is an example message window displayed by Program: Win32/WinSoftware. WinAntivirus:



Installation This program implements an installer or dropper program in order to place its files onto a computer. When the installer is run, it performs the actions listed below. It creates these file folders: %AllUsersProfile%\Application Data\salesmonitor\

SOURCE: <http://www.microsoft.com/security/portal/Entry.aspx?Name=Program%3aWin32%2fWinSoftware.WinAntiVirus>

Program:Win32/WinSoftware.WinAntiVirus

Also Known As:

Win-Trojan/Winfixer.88272 (AhnLab)
W32/Backdoor.ATJS (Authentium (Command))
WinFixer.AZ (AVG)
Trojan.Downloader.Winfixer.O (BitDefender)
Win32/Adware.WinFixer (ESET)
Downloader.Win32.WinFixer.o (Kaspersky)
WinFixer (McAfee)
W32/WinFixer.GV (Norman)
Application/Winantivirus2006 (Panda)
WinSoftware Corporation (Sunbelt Software)
ErrorSafe (Symantec)
TROJ_DLOADER.EWR (Trend Micro)

Summary

Program:Win32/WinSoftware is a program that displays warnings or malware detections, in order to prompt users to purchase WinAntiVirus.

Symptoms

The following symptoms may indicate the presence of Program:Win32/WinSoftware.WinAntiVirus:

- An uninstaller entry for WinAntiVirus in the "Add or Remove Programs" list.
- A "WinAntiVirus" entry under the Programs section of the user's **Start Menu**.

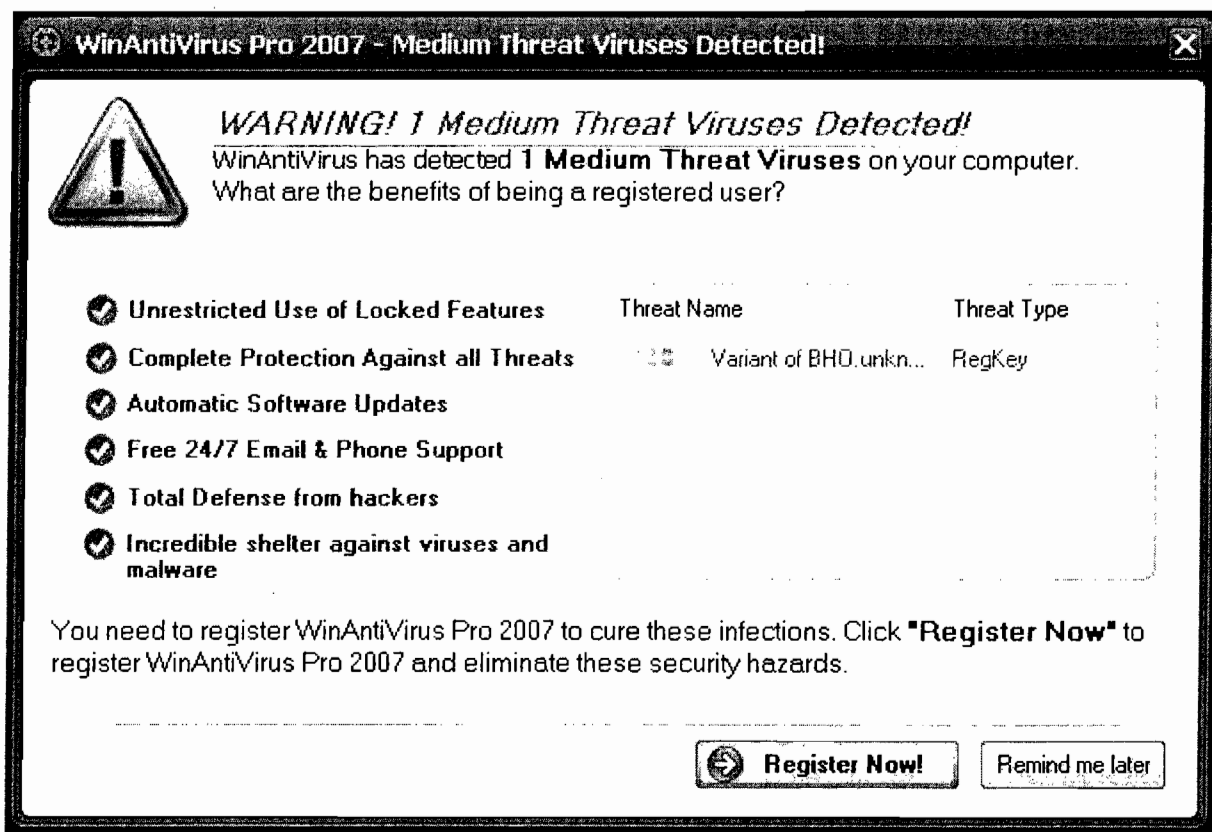
- A "WinAntiVirus" icon in the system tray, resembling the following graphic :



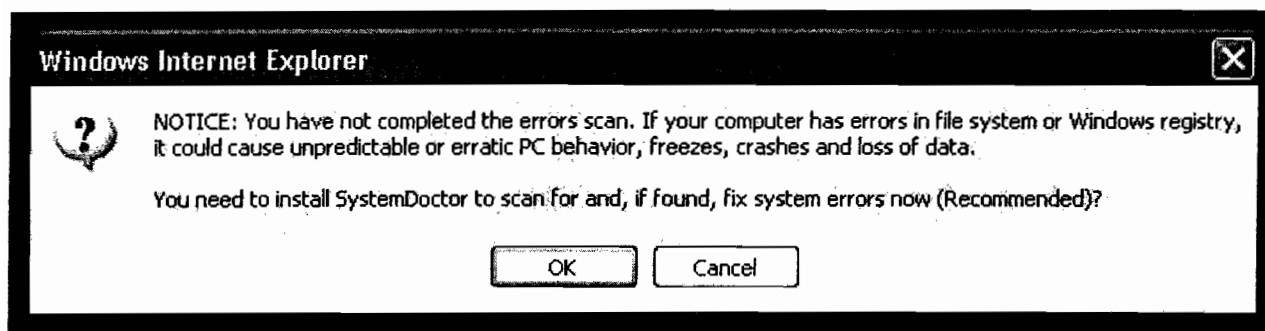
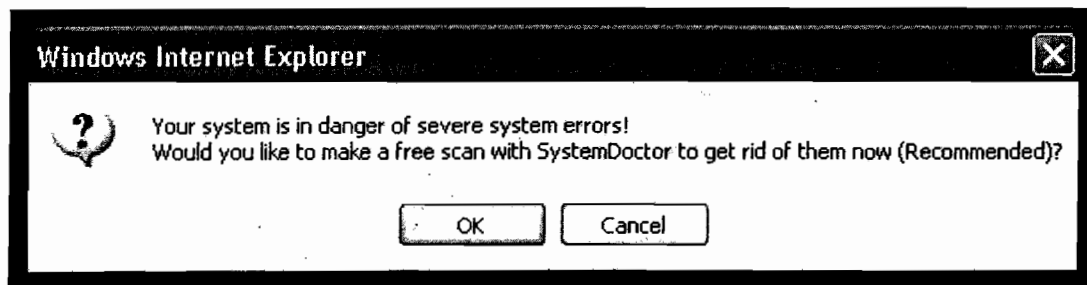
- An application shortcut named WinAntiVirus on the desktop, resembling the following graphic.



- The appearance of a dialog box resembling the graphic below; the dialog box warns that the system is infected and prompts the user to purchase WinAntiVirus to clean the system.



- The appearance of dialog boxes resembling the two below; these dialog boxes warn that the system is in danger due to severe system errors and prompts the user to install a program mentioned as 'SystemDoctor' to clean the system:





Microsoft.com

Search Microsoft.com

Go

Powered by

[Top Detections](#) [Encyclopedia](#) [Tools & Resources](#) [Submit a Sample](#)

Microsoft® Malware Protection Center

Threat Research and Response



NOTICE: October 23, 2008: Today the MSRC released Security Bulletin MS08-067. For more information on this bulletin, and to stay protected get the latest information from the MMPC here on our blog.

Program: Win32/DriveCleaner

[Summary](#)[Analysis](#)[Prevention](#)[Recovery](#)

Also Known As:

DriveCleaner (McAfee)
W32/WinFixer.NU (Norman)
DriveCleaner (Sunbelt Software)
DriveCleaner (Symantec)
FreeIoa.8F4CBEAA (Trend Micro)

Summary

Program:Win32/DriveCleaner locates various registry entries, Windows prefetch content, Windows recently accessed files and other types of data, and identifies them as "Privacy Violations". DriveCleaner then prompts the user to purchase the product in order to remove the alleged 'violations'.

Symptoms

The following may be symptoms of a DriveCleaner installation:

- Presence of an icon on the desktop such as the following:



- Presence of an icon in the Quick Launch toolbar such as the following:



- Presence of an entry named "DriveCleaner Free" or similar in 'Add or Remove Programs'
- Presence of registry value names:
 - DriveCleaner Free
 - SDR6_Check
 - UDC6cw
 - PAS_Check
 - Dnsein registry subkey:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Presence of the following files:
 - %ProgramFiles%\DriveCleaner Free\udc.exe
 - %ProgramFiles%\DriveCleaner Free\udcpchk.dll
 - %ProgramFiles%\DriveCleaner Free\insthelp.exe
 - %ProgramFiles%\DriveCleaner Free\udc6cw.exe
 - %ProgramFiles%\DriveCleaner Free\pv.exe
 - %Temp%\udc6_0001_d21m1601\installer.exe

[Search the Encyclopedia](#)

Latest Definition Updates

Windows Defender
Antispyware: v1.45.1198.0

- 32 bit
- 64 bit
- Information on updating Windows Defender

Microsoft Forefront Client Security
Antivirus: v1.45.1198.0
Antispyware: v1.45.1198.0

- 32 bit
- 64 bit
- Information on updating Microsoft Forefront Client Security

Severity

- ☒ High
- ☐ Medium
- ☐ Low

Glossary

[View the Glossary](#)



[Free Security Newsletter](#) | [Contact Microsoft](#) | [MMPC Portal Feedback](#)

[Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)
© 2007 Microsoft Corporation. All rights reserved.



One step ahead.

[Panda Worldwide](#) [About Panda](#) [Contact](#)**Home Users**[Enterprises](#)[Partners](#)[Products](#) [Downloads](#) [Store](#) [Support](#) [Security Info](#) [Press Center](#)[Home](#) [Home Users](#) [Security Info](#) [Encyclopedia](#)**Security Info****Latest Threats****Cybercrime**[Spyware](#)
[Phishing](#)
[Spam](#)
[Others](#)**Classic Malware**[Virus](#)
[Worms](#)
[Trojans](#)
[Others](#)**Mobile-Threats****Tools and Resources**[Malware Search Engine](#)
[Are you really protected?](#)
[PandaLabs Reports](#)
[Glossary](#)**Blog PandaLabs****New 2009 product line
Renew now!****Encyclopedia****Winfixer2005****Threat Level** ■■■ **Damage** ■■ **Distribution** ■■■[At a glance](#) | [Tech details](#) | [Solution](#)

Common name:	Winfixer2005
Technical name:	Application/Winfixer2005
Threat level:	Low
Alias:	WinSoftware.com,
Type:	Potentially Unwanted Program (PUP)
Effects:	It scans the computer in search of supposed errors in the <i>Windows Registry</i> and the hard disk, and of supposedly damaged files. Then, the user has to register in its website in order to repair them.
Affected platforms:	Windows 2003/XP/2000/NT/ME/98
First detected on:	Sept. 20, 2005
Detection updated on:	Oct. 31, 2007
Statistics	No
Proactive protection:	Yes, using TruPrevent Technologies

Brief Description

Winfixer2005 belongs to the category of Potentially Unwanted Programs, also known as PUPs.

Winfixer2005 scans the affected computer in search of supposed errors in the *Windows Registry* and the hard disk, and of supposedly damaged files. Then, in order to repair them, the user has to register in its website.

Winfixer2005 can be voluntarily downloaded from the website belonging to the company that has developed it.

Visible Symptoms

Winfixer2005 is easy to recognize once it has affected the computer, as it creates the following shortcut in the *Desktop*:



Last updated: 31/10/2007

Virus News

01/03/08.-Trojans: the leading cyber-threat in 2007

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

[+ Noticias]

[Rate this website](#) | [Web Map](#) | [Contact Panda](#)© Panda Security 2008 | [Privacy policy](#) | [Legal notice](#)

Means of transmission

Further Details

Last updated: 31/10/2007

Virus News

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

[+ Noticias]



One step ahead.

Panda Worldwide About Panda Contact

Home Users

Enterprises

Partners

Products Downloads Store Support Security Info Press Center

Home Home Users Security Info Encyclopedia



Security Info

Latest Threats

Cybercrime

Spyware
Phishing
Spam
Others

Classic Malware

Virus
Worms
Trojans
Others

Mobile-Threats

Tools and Resources

Malware Search Engine
Are you really protected?
PandaLabs Reports
Glossary

Blog PandaLabs



Encyclopedia

WinFixer2006

Threat Level *** Damage **** Distribution *

At a glance

Tech details | Solution

Common name:	WinFixer2006
Technical name:	Application/WinFixer2006
Threat level:	Medium
Type:	Potentially Unwanted Program (PUP)
Effects:	It is a Potentially Unwanted Program, which can affect the users' consent, awareness or control over the program. It does not spread automatically using its own means.
Affected platforms:	MS-DOS; Windows 2003/XP/2000/NT/ME/98/95/3.X; IIS
First detected on:	Oct. 7, 2006
Detection updated on:	March 21, 2008
Statistics	No
Proactive protection:	Yes, using TruPrevent Technologies

Brief Description

WinFixer2006 belongs to the category of Potentially Unwanted Programs, also known as PUPs.

PUPs are programs that, due to their features or means of distribution, can affect users' consent, awareness or control over operations like:

- ❑ Installation.
- ❑ Modifications carried out on the computer.
- ❑ Behavior of the program.
- ❑ Processing of personal data.
- ❑ Uninstallation.

The evaluation criteria of PUPs are based on the proposals suggested by the Anti-Spyware Coalition, organization of which Panda Security is a member.

WinFixer2006 does not spread automatically using its own means. It needs an attacking user's intervention in order to reach the affected computer. The means of transmission used include, among others, floppy disks, CD-ROMs, email messages with attached files, Internet downloads, FTP, IRC channels, peer-to-peer (P2P) file sharing networks, etc.

Last updated: 21/03/2008

Virus News

01/03/08.-Trojans: the leading cyber-threat in 2007

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

[+ Noticias]

Rate this website | Web Map | Contact Panda

© Panda Security 2008 | Privacy policy | Legal notice



One step ahead.

[Panda Worldwide](#) [About Panda](#) [Contact](#)**Home Users**[Enterprises](#)[Partners](#)[Products](#) [Downloads](#) [Store](#) [Support](#) [Security Info](#) [Press Center](#)[Home](#) [Home Users](#) [Security Info](#) [Encyclopedia](#)**Security Info****Latest Threats****Cybercrime**[Spyware](#)
[Phishing](#)
[Spam](#)
[Others](#)**Classic Malware**[Virus](#)
[Worms](#)
[Trojans](#)
[Others](#)**Mobile-Threats****Tools and Resources**[Malware Search Engine](#)
[Are you really protected?](#)
[PandaLabs Reports](#)
[Glossary](#)**Blog PandaLabs****New 2009 product line
Renew now!****Encyclopedia****WinFixer2006****Threat Level** *** **Damage** **** **Distribution** *[At a glance](#) [Tech details](#) [Solution](#)**Effects**

WinFixer2006 belongs to the category of Potentially Unwanted Programs, also known as PUPs.

PUPs are programs that, due to their features or means of distribution, can affect users' consent, awareness or control over operations like:

- ▣ Installation.
- ▣ Modifications carried out on the computer.
- ▣ Behavior of the program.
- ▣ Processing of personal data.
- ▣ Uninstallation.

The evaluation criteria of PUPs are based on the proposals suggested by the Anti-Spyware Coalition, organization of which Panda Security is a member.

Means of transmission

WinFixer2006 does not spread automatically using its own means. It needs the attacking user's intervention in order to reach the affected computer. The means of transmission used include, among others, floppy disks, CD-ROMs, email messages with attached files, Internet downloads, FTP, IRC channels, peer-to-peer (P2P) file sharing networks, etc.

Further Details

WinFixer2006 has the following additional characteristics:

- ▣ It is 45525 bytes in size.
- ▣ It is compressed with Upack.

Last updated: 21/03/2008

Virus News

01/03/08.-Trojans: the leading cyber-threat in 2007

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

[+ Noticias]

[Rate this website](#) | [Web Map](#) | [Contact Panda](#)

© Panda Security 2008 | [Privacy policy](#) | [Legal notice](#)



One step ahead.

[Panda Worldwide](#) [About Panda](#) [Contact](#)[Home Users](#)[Enterprises](#)[Partners](#)[Products](#) [Downloads](#) [Store](#) [Support](#) [Security Info](#) [Press Center](#)[Home](#) [Home Users](#) [Security Info](#) [Encyclopedia](#)**Security Info****Latest Threats****Cybercrime**[Spyware](#)[Phishing](#)[Spam](#)[Others](#)**Classic Malware**[Virus](#)[Worms](#)[Trojans](#)[Others](#)**Mobile-Threats****Tools and Resources**[Malware Search Engine](#)[Are you really protected?](#)[PandaLabs Reports](#)[Glossary](#)**Blog PandaLabs****New 2009 product line
Renew now!****Encyclopedia****AdvancedCleaner****Threat Level** **Damage** **Distribution**[At a glance](#) [Tech details](#) [Solution](#)

Common name:	AdvancedCleaner
Technical name:	Adware/AdvancedCleaner
Threat level:	Medium
Type:	Adware
Effects:	It does not spread automatically using its own means.
Affected platforms:	Windows 2003/XP/2000/NT/ME/98/95
First detected on:	Jan. 26, 2008
Detection updated on:	Jan. 27, 2008
Statistics	No
Proactive protection:	Yes, using TruPrevent Technologies

Brief Description

Adware refers to programs that display advertising using any means: pop-ups, banners, changes to the browser home page or search page, etc. The advertisements could be associated with the products or services offered by the creator of the program or by third-parties.

Adware can be installed in a number of ways, on some occasions without users' consent, and either with or without users' knowledge of its function.

AdvancedCleaner does not spread automatically using its own means. It needs an attacking user's intervention in order to reach the affected computer. The means of transmission used include, among others, floppy disks, CD-ROMs, email messages with attached files, Internet downloads, FTP, IRC channels, peer-to-peer (P2P) file sharing networks, etc.

Last updated: 27/01/2008

Virus News

01/03/08.-Trojans: the leading cyber-threat in 2007

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

[\[+ Noticias\]](#)[Rate this website](#) [Web Map](#) [Contact Panda](#)[Panda Security 2008](#) [Privacy policy](#) [Legal notice](#)

*One step ahead.***Home Users**

Enterprises

Partners

[Products](#) · [Downloads](#) · [Store](#) · [Support](#) · [Security Info](#) · [Press Center](#)[Home](#) · [Home Users](#) · [Security Info](#) · [Encyclopedia](#)**Security Info****Latest Threats****Cybercrime**[Spyware](#)
[Phishing](#)
[Spam](#)
[Others](#)**Classic Malware**[Virus](#)
[Worms](#)
[Trojans](#)
[Others](#)**Mobile-Threats****Tools and Resources**[Malware Search Engine](#)
[Are you really protected?](#)
[PandaLabs Reports](#)
[Glossary](#)**Blog PandaLabs****New 2009 product line
Renew now!****Encyclopedia****AdvancedCleaner****Threat Level** ■ **Damage** ■ ■ ■ **Distribution** ■ ■ ■[At a glance](#) [Tech details](#) [Solution](#)**Effects****Means of transmission**

AdvancedCleaner does not spread automatically using its own means. It needs the attacking user's intervention in order to reach the affected computer. The means of transmission used include, among others, floppy disks, CD-ROMs, email messages with attached files, Internet downloads, FTP, IRC channels, peer-to-peer (P2P) file sharing networks, etc.

Further Details

AdvancedCleaner has the following additional characteristics:

- ▣ It is 5120 bytes in size.

Last updated: 27/01/2008

Virus News

01/03/08.-Trojans: the leading cyber-threat in 2007

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

[\[+ Noticias\]](#)[Rate this website](#) | [Web Map](#) | [Contact Panda](#)© Panda Security 2008 | [Privacy policy](#) | [Legal notice](#)



One step ahead.

Panda Worldwide About Panda Contact

Home Users

Enterprises

Partners

Products Downloads Store Support Security Info Press Center

Home Home Users Security Info Encyclopedia



Security Info

Latest Threats

Cybercrime

Spyware
Phishing
Spam
Others

Classic Malware

Virus
Worms
Trojans
Others

Mobile-Threats

Tools and Resources

Malware Search Engine
Are you really protected?
PandaLabs Reports
Glossary

Blog PandaLabs

New 2009 product line
Renew now!

Encyclopedia

AdvancedCleaner

Threat Level ■ Damage ■ Distribution ■

At a glance Tech details Solution

Common name:	AdvancedCleaner
Technical name:	Application/AdvancedCleaner
Threat level:	Medium
Type:	Adware
Effects:	It displays pop-up messages when it runs, distracting users and affecting productivity. It spreads , across the Internet.
Affected platforms:	Windows 2003/XP/2000/NT/ME/98/95
First detected on:	April 7, 2008
Detection updated on:	April 30, 2008
Statistics	No

Brief Description

Adware refers to programs that display advertising using any means: pop-ups, banners, changes to the browser home page or search page, etc. The advertisements could be associated with the products or services offered by the creator of the program or by third-parties.

Adware can be installed in a number of ways, on some occasions without users' consent, and either with or without users' knowledge of its function.

It affects productivity, preventing tasks from being carried out:

- In the affected computer: it displays pop-up windows.

AdvancedCleaner uses the following propagation or distribution methods:

- Exploiting vulnerabilities with the intervention of the user: exploiting vulnerabilities in file formats or applications. To exploit them successfully it needs the intervention of the user: opening files, viewing malicious web pages, reading emails, etc.
- Via Internet, exploiting remote vulnerabilities: attacking random IP addresses, in which it tries to insert a copy of itself by exploiting one or more vulnerabilities.

Last updated: 30/04/2008

Virus News

01/03/08.-Trojans: the leading cyber-threat in 2007

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

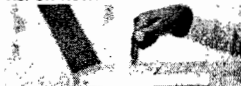
[+ Noticias]

Rate this website | Web Map | Contact Panda

© Panda Security 2008 | Privacy policy | Legal notice



One step ahead.

[Panda Worldwide](#) [About Panda](#) [Contact](#)[Home Users](#)[Enterprises](#)[Partners](#)[Products](#) [Downloads](#) [Store](#) [Support](#) [Security Info](#) [Press Center](#)[Home](#) [Home Users](#) [Security Info](#) [Encyclopedia](#)**Security Info****Latest Threats****Cybercrime**[Spyware](#)
[Phishing](#)
[Spam](#)
[Others](#)**Classic Malware**[Virus](#)
[Worms](#)
[Trojans](#)
[Others](#)**Mobile-Threats****Tools and Resources**[Malware Search Engine](#)
[Are you really protected?](#)
[PandaLabs Reports](#)
[Glossary](#)**Blog PandaLabs****New 2009 product line
Renew now!****Encyclopedia****AdvancedCleaner****Threat Level** ■■■ **Damage** ■■ **Distribution** ■[At a glance](#) [Tech details](#) [Solution](#)**Effects**

It affects productivity, preventing tasks from being carried out:

- It displays pop-up windows.

Means of transmission**Propagation through the exploits of remote vulnerabilities:***AdvancedCleaner* carries out the following process:

- It spreads by attacking IP addresses obtained at random or from the network to which the infected computer belongs.
- It tries to access the IP addresses under attack by exploiting an existing vulnerability or through an open port.
- If it does this, it downloads a copy of itself onto the vulnerable computer.

Further Details*AdvancedCleaner* has the following additional characteristics:

- It is 4963616 bytes in size.

Last updated: 30/04/2008

Virus News

01/03/08.-Trojans: the leading cyber-threat in 2007

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

[\[+ Noticias\]](#)[Rate this website](#) | [Web Map](#) | [Contact Panda](#)© Panda Security 2008 | [Privacy policy](#) | [Legal notice](#)



One step ahead.

Panda Worldwide About Panda Contact

Home Users

Enterprises

Partners

Products Downloads Store Support Security Info Press Center

Home Home Users Security Info Encyclopedia



Security Info

Latest Threats

Cybercrime

Spyware

Phishing

Spam

Others

Classic Malware

Virus

Worms

Trojans

Others

Mobile-Threats

Tools and Resources

Malware Search Engine

Are you really protected?

PandaLabs Reports

Glossary

Blog PandaLabs



Encyclopedia

DriveCleaner

Threat Level Damage Distribution

At a glance

Tech details

Common name:	DriveCleaner
Technical name:	Application/DriveCleaner
Threat level:	Medium
Alias:	DriveCleaner,
Type:	Potentially Unwanted Program (PUP)
Effects:	It is a Potentially Unwanted Program, which can affect the users' consent, awareness or control over the program. It notifies the attacker that the computer has been compromised and is ready to be used maliciously. It spreads , across the Internet.
Affected platforms:	Windows 2003/XP/2000/NT/ME/98/95
First detected on:	July 30, 2006
Detection updated on:	Sept. 8, 2007
Statistics	No
Proactive protection:	Yes, using TruPrevent Technologies

Brief Description

DriveCleaner belongs to the category of Potentially Unwanted Programs, also known as PUPs.

PUPs are programs that, due to their features or means of distribution, can affect users' consent, awareness or control over operations like:

- ▣ Installation.
- ▣ Modifications carried out on the computer.
- ▣ Behavior of the program.
- ▣ Processing of personal data.
- ▣ Uninstallation.

The evaluation criteria of PUPs are based on the proposals suggested by the Anti-Spyware Coalition, organization of which Panda Security is a member.

It reduces the security level of the computer: it notifies the attacker that the computer has been compromised and is ready to be used maliciously.

DriveCleaner uses the following propagation or distribution methods:

- ▣ Exploiting vulnerabilities with the intervention of the user: exploiting vulnerabilities in file formats or applications. To exploit them successfully it needs the intervention of the user: opening files, viewing malicious web pages, reading emails, etc.
- ▣ Via Internet, exploiting remote vulnerabilities: attacking random IP addresses, in which it tries to insert a copy of itself by exploiting one or more vulnerabilities.
- ▣ It is dropped or downloaded to the computer by other malware specimens, for example: Downloader.PAG.

Last updated: 06/09/2007

Virus News

01/03/08.-Trojans: the leading cyber-threat in 2007

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

[+ Noticias]

Rate this website | Web Map | Contact Panda

© Panda Security 2008 | Privacy policy | Legal notice



One step ahead.

[Panda Worldwide](#) [About Panda](#) [Contact](#)**Home Users**[Enterprises](#)[Partners](#)[Products](#) [Downloads](#) [Store](#) [Support](#) [Security Info](#) [Press Center](#)[Home](#) [Home Users](#) [Security Info](#) [Encyclopedia](#)**Security Info****Latest Threats****Cybercrime**[Spyware](#)
[Phishing](#)
[Spam](#)
[Others](#)**Classic Malware**[Virus](#)
[Worms](#)
[Trojans](#)
[Others](#)**Mobile-Threats****Tools and Resources**[Malware Search Engine](#)
[Are you really protected?](#)
[PandaLabs Reports](#)
[Glossary](#)**Blog PandaLabs****Encyclopedia****DriveCleaner****Threat Level** **Damage** **Distribution**[At a glance](#) [Tech details](#) [Solution](#)**Effects**

DriveCleaner is a Potentially Unwanted Program, also known as PUP.

Due to their features or means of distribution, these programs can affect users' consent, awareness or control over operations like:

- ▣ Installation.
- ▣ The modifications carried out on the computer.
- ▣ The behavior of the program.
- ▣ The way user's personal data is processed.
- ▣ Uninstallation.

The evaluation criteria of PUPs are based on the proposals suggested by the Anti-Spyware Coalition, organization of which Panda Security is a member.

It reduces the security level of the computer:

- ▣ It notifies the attacker that the computer has been compromised and is ready to be used maliciously.

Means of transmission**Propagation through the exploits of remote vulnerabilities:**

DriveCleaner carries out the following process:

- ▣ It spreads by attacking IP addresses obtained at random or from the network to which the infected computer belongs.
- ▣ It tries to access the IP addresses under attack by exploiting an existing vulnerability or through an open port.
- ▣ If it does this, it downloads a copy of itself onto the vulnerable computer.

Further Details

DriveCleaner has the following additional characteristics:

- ▣ It is written in the programming language Visual C++ 7.
- ▣ It is 143056 bytes in size.
- ▣ It is compressed with unknown.

Last updated: 03/09/2007

Virus News

01/03/08.-Trojans: the leading cyber-threat in 2007

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

[+ Noticias]

[Rate this website](#) | [Web Map](#) | [Contact Panda](#)

[Panda Security 2008](#) | [Privacy policy](#) | [Legal notice](#)



One step ahead.

Panda Worldwide About Panda Contact

Home Users

Enterprises

Partners

Products Downloads Store Support Security Info Press Center

Home » Home users » Security Info » Encyclopedia



Security Info

Latest Threats

Cybercrime

Spyware
Phishing
Spam
Others

Classic Malware

Virus
Worms
Trojans
Others

Mobile-Threats

Tools and Resources

Malware Search Engine
Are you really protected?
PandaLabs Reports
Glossary

Blog PandaLabs

New 2009 product line
Renew now!

Encyclopedia

DriveCleaner

Threat Level ■■■ Damage ■■■ Distribution ■

At a glance Tech details Solution

Common name:	DriveCleaner
Technical name:	Adware/DriveCleaner
Threat level:	Low
Alias:	Alphabet.gen,
Type:	Spyware
Subtype:	Adware
Effects:	It collects information on Internet usage and the applications installed in the computer and uses it to display pop-up advertisements.
Affected platforms:	Windows 2003/XP/2000/NT/ME/98/95
First detected on:	Dec. 2, 2006
Detection updated on:	April 25, 2008
Statistics	No
Proactive protection:	Yes, using TruPrevent Technologies

Brief Description

Adware refers to programs that display advertising using any means: pop-ups, banners, changes to the browser home page or search page, etc. The advertisements could be associated with the products or services offered by the creator of the program or by third-parties.

Adware can be installed in a number of ways, on some occasions without users' consent, and either with or without users' knowledge of its function.

DriveCleaner uses the following propagation or distribution methods:

- Exploiting vulnerabilities with the intervention of the user: exploiting vulnerabilities in file formats or applications. To exploit them successfully it needs the intervention of the user: opening files, viewing malicious web pages, reading emails, etc.
- It is dropped or downloaded to the computer by other malware specimens, for example: Multidropper.REY, Multidropper.REZ, Downloader.NIW, Downloader.NMT, DisableKey, Downloader.OEP, Downloader.OES, Downloader.OVL, Downloader.OVO, Downloader.OYI, Downloader.PAP, Downloader.PLA, Downloader.PLN, Downloader.QEA.

Last updated: 25/04/2008

Virus News

01/03/08.-Trojans: the leading cyber-threat in 2007

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

[+ Noticias]

Rate this website | Web Map | Contact Panda

© Panda Security 2008 | Privacy policy | Legal notice



One step ahead.

[Panda Worldwide](#) [About Panda](#) [Contact](#)[Products](#) [Downloads](#) [Store](#) [Support](#) [Security Info](#) [Press Center](#) [Home Users](#) [Enterprises](#) [Partners](#)[Home](#) [Home Users](#) [Security Info](#) [Encyclopedia](#)**Security Info****Latest Threats****Cybercrime**[Spyware](#)[Phishing](#)[Spam](#)[Others](#)**Classic Malware**[Virus](#)[Worms](#)[Trojans](#)[Others](#)**Mobile-Threats****Tools and Resources**[Malware Search Engine](#)[Are you really protected?](#)[PandaLabs Reports](#)[Glossary](#)**Blog PandaLabs**

New 2009 product line
Renew now!

**Encyclopedia****DriveCleaner****Threat Level** ■■■■■ **Damage** ■■■■■ **Distribution** ■■■■■[At a glance](#) [Tech details](#) [Solution](#)**Effects**

DriveCleaner carries out the following actions:

- ▣ *DriveCleaner* displays advertising on the screen. The advertisements could be associated to the products or services offered by the creator of the program or third-parties.

Means of transmission

DriveCleaner does not spread automatically using its own means. It needs the attacking user's intervention in order to reach the affected computer. The means of transmission used include, among others, floppy disks, CD-ROMs, email messages with attached files, Internet downloads, FTP, IRC channels, peer-to-peer (P2P) file sharing networks, etc.

Further Details

DriveCleaner has the following additional characteristics:

- ▣ It is 72704 bytes in size.
- ▣ It is compressed with PecBundle, PECompact.

Last updated: 25/04/2008

Virus News

01/03/08.-Trojans: the leading cyber-threat in 2007

12/20/07.-Virus almanac 2007

12/19/07.-2008 will witness an avalanche of malware designed for stealing money, reports PandaLabs

[+ Noticias]

[Rate this website](#) | [Web Map](#) | [Contact Panda](#)

© Panda Security 2008 | [Privacy policy](#) | [Legal notice](#)



Spyware Information: WinFixer

This application is **adware**. Adware is not normally a threat, but is usually considered a nuisance. It might have been installed by another application. It can pop up advertisements even if you have a popup blocker on your computer. It can monitor your computer usage to generate ads that you are more likely to respond to. Adware can consume processing power and network bandwidth, thus slowing down your computer and interrupting your workflow.

- ④ Size: 2,234,435 bytes
- ④ Threat level: Medium (more info...)
- ④ Detections: 178,808 this month: 75
- ④ Author: WinSoftware
- ④ Others by this author: WinAntiVirus, WinAntiSpyware
- ④ Appeared: 7/25/2005

Research

- ④ **Method of infection:** WinFixer is usually installed by pop up ads displayed by other spyware. The ad is usually a Windows dialog box prompting to install WinFixer. It will inform the user that there are critical system problems and WinFixer should be downloaded immediatley. Even if the user selects the do not install option or closes the dialog, WinFixer will install itself regardless.
- ④ **Advertising:** Once installed, WinFixer will alert the user that there are many critical errors on the infected machine. It will then inform the user that they must register WinFixer immediatley to fix these problems.
- ④ **Privacy issues:** WinFixer may collect personally identifiable information and share that information with its affiliates. It may also gather information about the user's computer and could possibly report that back to its controlling servers.
- ④ **Privacy policy:** WinFixer Privacy Policy
- ④ **Security issues:** WinFixer will automatically install itself without permission, it may also allow for other unsigned executable code to be run without user permission.
- ④ **Stability issues:** WinFixer runs as a background process and installs files into the sytem directory. Because it runs as a background process and nests itself into the operating system it may cause degraded system performance among other things.

Spyware Detection Stats

- ④ Spyware Fingerprints: 91,859
- ④ Detections: 6,758,527
- ④ Detections this Month: 4,528

Spyware Search

Enter Spyware Name

Search

Recommended

Keep your computer safe. Automatically keeps up-to-date to protect from the latest threats.





[Shopping Cart](#) [Contact Us](#) [Site Map](#)

[Home](#) [Products](#) [Support](#) [Resources](#) [Community](#) [Buy](#) [Company](#) [Partners](#)



PARETO LABS

[DLL Lab](#)

[EXE Lab](#)

[Anti-Spyware Lab](#)

[Common Questions](#)

[Spyware Behavior](#)

[Types of Spyware](#)

[Safety Tips](#)

[Characteristics](#)

[Detection Criteria](#)

[Glossary / Definitions](#)

[Links](#)

[Technology](#)

[Anti-Virus Lab](#)

RELATED

[ParetoLogic Blogs](#)

WinAntiVirus Pro 2006

[back to Definitions list](#)

Infected with WinAntiVirus Pro 2006 ?

[Free Scan](#)

Description

WinAntiVirus is a program that lists false positives and pop-up advertisements in order to goad the user into purchasing the product. The program can be downloaded and installed without the users knowledge or consent by way of drive by downloads from certain sites. It also uses cookies to track browser activity and behaviour It is also associated with WinFixer.

Vendor

Winsoftware

Vendor URL

<http://www.winantivirus.com>

Threat Level: Severe Risk



WinAntiVirus Pro 2006 Characteristics

Displays ads	
Records personal data / keystrokes	
Hijacks internet browser	
Allows remote influence	
Downloads unsolicited files	●
Disables programs / system	
Makes unauthorized phone calls	
Exploits a security flaw	●
Floods internet connection	
Distributes threats	●
Tracks browsing activity with installed applications	
Tracks browsing activity with cookies	
Installs without user consent	
Inadequate uninstall procedures	
Insufficient privacy disclosure and consent	
Uses excessive system resources	
Makes fraudulent claims about spyware detection and removal	●
Performs Silent Updates	



applications from your computer quickly, powerfully and completely with XoftSpySE Anti-Spyware.

[Shopping Cart](#) [Contact Us](#) [Site Map](#)[Home](#)[Products](#)[Support](#)[Resources](#)[Community](#)[Buy](#)[Company](#)[Partners](#)

PARETO LABS

[DLL Lab](#)[EXE Lab](#)[Anti-Spyware Lab](#)[Common Questions](#)[Spyware Behavior](#)[Types of Spyware](#)[Safety Tips](#)[Characteristics](#)[Detection Criteria](#)[Glossary / Definitions](#)[Links](#)[Technology](#)[Anti-Virus Lab](#)

RELATED

[ParetoLogic Blogs](#)

WinAntiSpyware 2006

[back to Definitions list](#)

Infected with WinAntiSpyware 2006 ?

[Free Scan](#)**Description**

WinAntiSpyware is a program that lists false positives and pop-up advertisements in order to goad the user into purchasing the product. The program can be downloaded and installed without the users knowledge or consent by way of drive by downloads from certain sites. It also uses cookies to track browser activity and behaviour. It is also associated with WinFixer and WinAntiVirus.

Vendor

N/A

Vendor URL

N/A

Threat Level: Severe Risk**WinAntiSpyware 2006 Characteristics**

Displays ads	●
Records personal data / keystrokes	
Hijacks internet browser	
Allows remote influence	
Downloads unsolicited files	●
Disables programs / system	
Makes unauthorized phone calls	
Exploits a security flaw	
Floods internet connection	
Distributes threats	
Tracks browsing activity with installed applications	
Tracks browsing activity with cookies	●
Installs without user consent	●
Inadequate uninstall procedures	
Insufficient privacy disclosure and consent	●
Uses excessive system resources	
Makes fraudulent claims about spyware detection and removal	●
Performs Silent Updates	

Page 165

Attachment C

Remove WinAntiSpyware 2006



Remove WinAntiSpyware 2006 and other unwanted applications from your computer quickly, powerfully and completely with XoftSpySE Anti-Spyware.


[Shopping Cart](#) [Contact Us](#) [Site Map](#)
[Home](#) [Products](#) [Support](#) [Resources](#) [Community](#) [Buy](#) [Company](#) [Partners](#)


PARETO LABS

[DLL Lab](#)[EXE Lab](#)[Anti-Spyware Lab](#)[Common Questions](#)[Spyware Behavior](#)[Types of Spyware](#)[Safety Tips](#)[Characteristics](#)[Detection Criteria](#)[Glossary / Definitions](#)[Links](#)[Technology](#)[Anti-Virus Lab](#)

RELATED

[ParetoLogic Blogs](#)

WinFixer

[back to Definitions list](#)

Infected with WinFixer ?

[Free Scan](#)

Description

This application is a rogue security tool, a program that claims to detect and remove or disable spyware, viruses or other Internet threats. However, its capabilities are limited, and the tool may actually function as spyware or adware. WinFixer is a prevalent and frustrating rogue security tool that claims to find and remove Windows errors and security risks, but will merely prompt the user to purchase the full version, which has little value as a security or optimization tool.

Vendor

Its author is WinFixer.com

Vendor URL

<http://www.winfixer.com/>

Threat Level: Severe Risk



WinFixer Characteristics

Displays ads	●
Records personal data / keystrokes	
Hijacks internet browser	
Allows remote influence	
Downloads unsolicited files	
Disables programs / system	
Makes unauthorized phone calls	
Exploits a security flaw	
Floods internet connection	
Distributes threats	●
Tracks browsing activity with installed applications	
Tracks browsing activity with cookies	
Installs without user consent	
Inadequate uninstall procedures	
Insufficient privacy disclosure and consent	
Uses excessive system resources	
Makes fraudulent claims about spyware detection and removal	
Performs Silent Updates	

**Remove WinFixer**

Remove WinFixer and other unwanted applications from your computer quickly, powerfully and completely with XoftSpySE Anti-Spyware.

[Shopping Cart](#) [Contact Us](#) [Site Map](#)[Home](#)[Products](#)[Support](#)[Resources](#)[Community](#)[Buy](#)[Company](#)[Partners](#)

PARETO LABS

[DLL Lab](#)[EXE Lab](#)[Anti-Spyware Lab](#)[Common Questions](#)[Spyware Behavior](#)[Types of Spyware](#)[Safety Tips](#)[Characteristics](#)[Detection Criteria](#)[Glossary / Definitions](#)[Links](#)[Technology](#)[Anti-Virus Lab](#)

RELATED

[ParetoLogic Blogs](#)

DriveCleaner

[back to Definitions list](#)

Infected with DriveCleaner ?

[Free Scan](#)**Description**

DriveCleaner is a rogue application distributed through aggressive pop ups, typically after multiple infections.

Vendor

Winsoftware

Vendor URL

<http://www.drivecleaner.com>

Threat Level: Severe Risk**DriveCleaner Characteristics**

Displays ads	
Records personal data / keystrokes	
Hijacks internet browser	
Allows remote influence	
Downloads unsolicited files	
Disables programs / system	
Makes unauthorized phone calls	
Exploits a security flaw	●
Floods internet connection	
Distributes threats	
Tracks browsing activity with installed applications	
Tracks browsing activity with cookies	
Installs without user consent	
Inadequate uninstall procedures	
Insufficient privacy disclosure and consent	●
Uses excessive system resources	
Makes fraudulent claims about spyware detection and removal	●
Performs Silent Updates	

Remove DriveCleaner

Remove DriveCleaner and other unwanted applications from your computer quickly, powerfully and completely with XoftSpySE Anti-Spyware.



Spyware Research > Infections > RogueAntiSpyware.WinAntiSpyware

Details of the selected infection are shown below. This infection can be detected and cleaned using [Spyware Doctor](#).

Name: RogueAntiSpyware.WinAntiSpyware

Threat Level: Low



Description: WinAntiSpyware is a Rogue Anti-Spyware application which produces many detections that are not malicious in order to persuade the user into buying their product before they can remove these spurious detections.

Type: TT_RAS

Threat analysis: [Search ThreatExpert to view reports](#)

Removal: This infection can be removed using [Spyware Doctor](#).

At least one or more of the following fields may be indicated:

- **Name:** the name of the specific infection, as presented in the database.
- **Also known as:** other names by which this infection may be known.
- **Type:** the category to which the infection belongs. Refer to the [Glossary](#) for further details on infection types.
- **Variant:** the family of infections to which this infection belongs.
- **By:** the vendor of this infection.
- **Threat:** the [threat level](#) assigned to this infection.
- **Description:** a more detailed description of the infection. If the information is available, technical aspects and symptoms of this infection are described here.

[« Back](#)

Go to another page: [MRC Home](#), [Infection Database](#), [Threat Levels](#), [Glossary](#), [Malware Dispute Form](#), [Submit Spyware](#)

[Home](#)

[Download](#)

[Purchase](#)

[Support](#)

[Partners](#)

[Company](#)

[Contact](#)

Copyright © 1998-2008

PC Tools. All rights
Reserved.

[Privacy Policy](#) | [Legal Notice](#)

**ThreatExpert**[Sign In](#) | [Register](#)Search Reports: [Want to search threats?](#)[Home](#)[ThreatExpert Reports](#)[Tools](#)[Threat Browser](#)[Submit Sample](#)[About ThreatExpert](#)**Browse/Search All Reports**[Last 24 hours](#) | [7 days](#) | [30 days](#) | [All](#)
[Known Bad](#) | [Suspicious](#) | [All](#)**Search:**[Submit New Sample](#) >>


Results 1 - 20 of 24

Date	Risk	Origin	Findings
10/14/2008 11:40:34 AM	..	n/a	not-a-virus:AdWare.Win32.BHO.dha, WinAntiSpyware
10/8/2008 11:30:44 PM	..	n/a	Trojan-Downloader.Win32.FraudLoad.vcby, WinAntiSpyware, New Malware.aj..
10/8/2008 5:41:19 PM	..		not-a-virus:Downloader.Win32.WinFixer.u, WinFixer, Downloader-BAW.dr..
9/16/2008 8:16:59 PM	..	n/a	Trojan-Downloader.Win32.FraudLoad.vcby, New Malware.aj, Mal/Heuri-E..
9/12/2008 2:24:09 PM	..	n/a	Infostealer.Gampass, New Malware.aj
8/22/2008 5:19:06 AM	..		Trojan.Virantix.C, not-a-virus:FraudTool.Win32.XPSecurityCenter.b..
8/21/2008 7:12:45 AM	..	n/a	Trojan-Downloader.Win32.FraudLoad.vbev, New Malware.aj, Mal/Emogen-N..
7/30/2008 2:02:37 PM	..	n/a	New Malware.aj
7/30/2008 10:42:18 AM	..	n/a	New Malware.aj
7/25/2008 12:26:50 AM	..	n/a	WinAntiSpyware!sd6, Generic.dx
7/23/2008 3:16:42 PM	..	n/a	Adware.Agent.ZO, Rootkit.Renos.Gen.11, WinAntiSpyware!sd6, Generic.dx
7/22/2008 11:43:26 PM	..	n/a	WinAntiSpyware!sd6, Generic.dx
7/22/2008 10:57:46 AM	..	n/a	Trojan-Clicker.Win32.Agent.bfu, RogueAntiSpyware.DiscoSemErros, ErrClean..
7/22/2008 3:51:28 AM	..	n/a	Adware.Agent.ZO, Rootkit.Renos.Gen.11, Hacktool.Rootkit, FakeAlert-C.dr..
7/18/2008 5:19:57 AM	..	n/a	New Malware.aj
7/16/2008 7:47:58 PM	..	n/a	WinAntiSpyware!sd6, New Malware.aj
7/15/2008 9:17:43 AM	..	n/a	WinAntiSpyware!sd6, New Malware.aj
7/15/2008 8:21:46 AM	..	n/a	Trojan.Renos.Gen!Pac.10, Adware.Agent.ZO, Rootkit.Renos.Gen.11..
7/14/2008 3:55:57 AM	..	n/a	New Malware.aj
7/13/2008 1:21:39 AM	..	n/a	New Malware.aj

1 2 [Next](#) >

Spyware Research > Infections > RogueAntiSpyware.ErrorSafeFree

Details of the selected infection are shown below. This infection can be detected and cleaned using [Spyware Doctor](#).

Name:	RogueAntiSpyware.ErrorSafeFree
Threat Level:	Medium
Description:	 ErrorSafeFree is a rogue anti-spyware program which pretends to scan your computer and show severe system threats installed on it. After that it prompts you to buy this software.
Type:	TT_RAS
By:	WinSoftware
Threat analysis:	Search ThreatExpert to view reports
Removal:	This infection can be removed using Spyware Doctor .

At least one or more of the following fields may be indicated:

- **Name:** the name of the specific infection, as presented in the database.
- **Also known as:** other names by which this infection may be known.
- **Type:** the category to which the infection belongs. Refer to the [Glossary](#) for further details on infection types.
- **Variant:** the family of infections to which this infection belongs.
- **By:** the vendor of this infection.
- **Threat:** the [threat level](#) assigned to this infection.
- **Description:** a more detailed description of the infection. If the information is available, technical aspects and symptoms of this infection are described here.

[« Back](#)

Go to another page: [MRC Home](#), [Infection Database](#), [Threat Levels](#), [Glossary](#), [Malware Dispute Form](#), [Submit Spyware](#)

[Home](#)

[Download](#)

[Purchase](#)

[Support](#)

[Partners](#)

[Company](#)

[Contact](#)

Copyright © 1998-2008
PC Tools. All rights
Reserved.

[Privacy Policy](#) | [Legal Notice](#)

[Visit ThreatExpert web site](#) | [Close Report](#)**Submission Summary:**

Submission details:

- Submission received: 25 September 2008, 00:04:57
- Processing time: 4 min 30 sec
- Submitted sample:
File MD5: 0x3BBF8AAFE8E8F86D4D746FA99D68628
Filesize: 1,617,733 bytes

Summary of the findings:

What's been found	Severity Level
Capability to send out email message(s) with the built-in SMTP client engine.	3
Downloads/requests other files from Internet.	3
Contains characteristics of an identified security risk.	0000000000

Technical Details:




Possible Security Risk

ⓐ **Attention!** Characteristics of the following security risk was identified in the system:

Security Risk	Description
RogueAntiSpyware.WinAntiVirus	WinAntiVirus is a rogue anti-virus program from WinSoftware which has been known to be downloaded by some trojans. It claims to remove virus infections but instead shows detections of legitimate keys and files to urge users to buy its application. Removal of this software is advisable if it is not installed for a purpose.

❖ **Attention!** The following threat category was identified:

Threat Category	Description
	A spyware program that represents security risk for a local system



File System Modifications

■ The following files were created in the system:

[illegible]

[illegible]

 Notes:

- %DesktopDir% is a variable that refers to the file system directory used to physically store file objects on the desktop. A typical path is C:\Documents and Settings\[UserName]\Desktop.
- %Programs% is a variable that refers to the file system directory that contains the user's program groups. A typical path is C:\Documents and Settings\[UserName]\Start Menu\Programs.
- %ProgramFiles% is a variable that refers to the Program Files folder. A typical path is C:\Program Files.

☐ The following directories were created:

- [illegible]

 **Notes:**

- `%AppData%` is a variable that refers to the file system directory that serves as a common repository for application-specific data. A typical path is `C:\Documents and Settings\[UserName]\Application Data`.

Memory Modifications

There were new processes created in the system:

Process Name	Process Filename	Main Module Size
restart.exe	%ProgramFiles%\agent vkontakte\restart.exe	143,360 bytes
[filename of the sample #1]	[file and pathname of the sample #1]	196,608 bytes

Registry Modifications

④ The following Registry Key was created:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65958641-8AAC-4079-BECC-F2D182F0CBA9}

☐ The newly created Registry Values are:

- ```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7695B641-8ACC-4DAA-ACF8-6121C3E42896}
 DisplayName = "Vkontakte v1.10"
 UninstallString = "%ProgramFiles%\Agent V Kontakte\uninst.exe"
 DisplayIcon = "%ProgramFiles%\Agent V Kontakte\AgentVkontakte.exe"
 DisplayVersion = "v1.10"
 URLInfoAbout = "http://agentvkontakte.ru"
 Publisher = ""
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
 VKontakte = "%ProgramFiles%\agent vkontakte\agentvkontakte.exe"
```

 Other details

Analysis of the file resources indicate the following possible country of origin:

Russian Federation



▣ To mark the presence in the system, the following Mutex object was created:

- VKontakteClient\_AppManager\_server\_mutex

▣ The following Internet Connection was established:

| Server Name  | Server Port | Connect as User | Connection Password |
|--------------|-------------|-----------------|---------------------|
| vkontakte.ru | 80          | (null)          | (null)              |

▣ The following GET requests were made:

- faq.php
- faq.php?

▣ The data identified by the following URL was then requested from the remote web server:

- <http://agentvkontakte.ru/updates/version.txt>

▣ There was application-defined hook procedure installed into the hook chain (e.g. to monitor keystrokes). The installed hook is handled by the following module:

- %ProgramFiles%\agent vkontakte\agentvkontakte.exe

All content ("Information") contained in this report is the copyrighted work of ThreatExpert Ltd and its associated companies ("ThreatExpert") and may not be copied without the express permission of ThreatExpert.

The Information is provided on an "as is" basis. ThreatExpert disclaims all warranties, whether express or implied, to the maximum extent permitted by law, including the implied warranties that the Information is merchantable, of satisfactory quality, accurate, fit for a particular purpose or need, or non-infringing, unless such implied warranties are legally incapable of exclusion. Further, ThreatExpert does not warrant or make any representations regarding the use or the results of the use of the Information in terms of their correctness, accuracy, reliability, or otherwise.

Copyright © 2008 ThreatExpert. All rights reserved.

## Spyware Research > Infections > RogueAntiSpyware.AdvancedCleaner

Details of the selected infection are shown below. This infection can be detected and cleaned using [Spyware Doctor](#).

|                         |                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name:</b>            | RogueAntiSpyware.AdvancedCleaner                                                                                                                                                                       |
| <b>Threat Level:</b>    | High                                                                                                                                                                                                   |
| <b>Description:</b>     | RogueAntiSpyware.AdvancedCleaner displays fake alerts in malware payloads in order to persuade users into buying the rogue antispyware products. It also comes bundled with RogueAntiSpyware.ErrClean. |
| <b>Threat analysis:</b> | <a href="#">Search ThreatExpert to view reports</a>                                                                                                                                                    |
| <b>Removal:</b>         | This infection can be removed using <a href="#">Spyware Doctor</a> .                                                                                                                                   |

At least one or more of the following fields may be indicated:

- **Name:** the name of the specific infection, as presented in the database.
- **Also known as:** other names by which this infection may be known.
- **Type:** the category to which the infection belongs. Refer to the [Glossary](#) for further details on infection types.
- **Variant:** the family of infections to which this infection belongs.
- **By:** the vendor of this infection.
- **Threat:** the [threat level](#) assigned to this infection.
- **Description:** a more detailed description of the infection. If the information is available, technical aspects and symptoms of this infection are described here.

[« Back](#)

Go to another page: [MRC Home](#), [Infection Database](#), [Threat Levels](#), [Glossary](#), [Malware Dispute Form](#), [Submit Spyware](#)

[Home](#)

[Download](#)

[Purchase](#)

[Support](#)

[Partners](#)

[Company](#)

[Contact](#)

Copyright © 1998-2008  
PC Tools. All rights  
Reserved.

[Privacy Policy](#) | [Legal Notice](#)

**ThreatExpert**[Sign In](#) | [Register](#)Search Reports: [Want to search threats?](#)[Home](#)[ThreatExpert Reports](#)[Tools](#)[Threat Browser](#)[Submit Sample](#)[About ThreatExpert](#)**Browse/Search All Reports**[Last 24 hours](#) | [7 days](#) | [30 days](#) | [All](#)[Known Bad](#) | [Suspicious](#) | [All](#)**Search:**[Submit New Sample](#) >>

Results 1 - 11 of 11

| Date                 | Risk | Origin | Findings                                                                       |
|----------------------|------|--------|--------------------------------------------------------------------------------|
| 6/27/2008 8:25:18 AM | ...  |        | RogueAntiSpyware.AdvancedCleaner                                               |
| 6/18/2008 8:20:11 PM | ...  |        | RogueAntiSpyware.AdvancedCleaner, Downloader, Downloader-BHW, TROJ_DLOADER.HGF |
| 6/2/2008 10:52:24 PM | ...  |        | RogueAntiSpyware.AdvancedCleaner, AdvancedCleaner                              |
| 5/31/2008 7:58:38 AM | ...  |        | RogueAntiSpyware.AdvancedCleaner                                               |
| 5/29/2008 1:46:57 AM | ...  |        | RogueAntiSpyware.AdvancedCleaner                                               |
| 5/20/2008 7:46:30 PM | ...  |        | RogueAntiSpyware.AdvancedCleaner                                               |
| 5/19/2008 3:07:01 PM | ...  | n/a    | RogueAntiSpyware.AdvancedCleaner, AdvancedCleaner..                            |
| 5/18/2008 6:55:39 AM | ...  |        | RogueAntiSpyware.AdvancedCleaner                                               |
| 5/15/2008 4:36:49 PM | ...  |        | RogueAntiSpyware.AdvancedCleaner                                               |
| 5/6/2008 7:43:01 AM  | ...  |        | RogueAntiSpyware.AdvancedCleaner                                               |
| 5/3/2008 3:28:17 AM  | ...  | n/a    | Win32.Trats.Gen, W32/Trats, PE_TRATS.E, RogueAntiSpyware.AdvancedCleaner..     |

**SOPHOS**

Welcome Login | Register

Global websites | Press | Contact us

**Troj/FakeVir-AA****Category**

» Viruses and Spyware

**Type**

» Trojan

**What to do**

» If you've received an alert for a virus or spyware, then follow the instructions for removing the threat.

**Prevalence**low  high**Summary****Affected operating systems**

Windows

**Included in our products from**

May 2007 (4.17)

**Protection available since**

19 March 2007 06:15:58 (GMT)

**Detected by**

All Sophos products

**Action**

Please follow the instructions for removing Trojans.

**More Information**

Troj/FakeVir-AA is a Trojan downloader for the Windows platform.

The Trojan displays fake spyware alerts to try and lure the user into installing software from a remote location. The alert is displayed in the form of the following message:

"Warning!

Trojan Adware.W32.ExpDwnldr spyware detected. This Trojan allows attackers to access your computer from remote locations, stealing passwords, Internet banking and personal data. This also prompts advertising popups.

This process is a security risk and should be removed from your system.

System Affected: Windows 98, 2000, NT, ME, XP

Security Risk(0-5): 4

Recommendations: Click Yes to get all available antispyware software."

When run Troj/FakeVir-AA creates the following files:

<Desktop>\PrivacyProtector.url

<Desktop>\SystemDoctor.url

<Desktop>\WinAntiSpyware 2007.url

These files can be safely removed.

Once installed, Troj/FakeVir-AA puts an icon in the system tray area. From this icon a balloon message is periodically displayed:

System detected virus activities. These may impact the performance of your computer. Please, use recommended antispyware software to protect your system from parasite programs.

When the balloon message or tray icon is clicked, a browser is opened and directed to a preconfigured website.

# SOPHOS

Welcome Login | Register

Global websites | Press | Contact us



## Troj/FakeVir-ES

### Aliases

FraudTool.Win32.WinAntiVirus.aj  
XPantivirus

### Category

› Viruses and Spyware

### Type

› Trojan

### What to do

› If you've received an alert for a virus or spyware, then follow the instructions for removing the threat.

### Prevalence

low  high

## Summary

### Affected operating systems

Windows

### Included in our products from

October 2008 (4.34)

### Protection available since

13 August 2008 22:43:13 (GMT)

### Detected by

All Sophos products

## Action

Please follow the instructions for removing Trojans.

## More Information

Troj/FakeVir-ES claims to be an anti-virus scanner called "WinProtector".

Troj/FakeVir-ES scans the computer and falsely reports presence of malware infections on the computer. Troj/FakeVir-ES then persistently prompts the user to purchase the full version of "WinProtector" in order to cleanup the infections.

When first run Troj/FakeVir-ES creates the following files:

<Program files>\WinProtector3.8\WinProtector.exe - copy of self  
<Program files>\NetFilter\netfilter.dll - also detected as Troj/FakeVir-ES

Registry entries are created under:

HKCU\Software\WinProtector  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WinProtector

# SOPHOS

[Welcome](#) [Login](#) | [Register](#)[Global websites](#) | [Press](#) | [Contact us](#)

## Troj/FakeVir-AZ

**Aliases**

Winfixer

**Category**

▸ Viruses and Spyware

**Type**

▸ Trojan

**What to do**

▸ If you've received an alert for a virus or spyware, then follow the instructions for removing the threat.

**Prevalence**low  high

### Summary

**Affected operating systems**

Windows

**Characteristics**

▪ Installs itself in the registry

**Included in our products from**

June 2008 (4.30)

**Protection available since**

26 April 2008 14:39:47 (GMT)

**Detected by**

All Sophos products

### Action

Please follow the instructions for removing Trojans.

### More Information

Troj/FakeVir-AZ claims to be a malware removal tool named "AntiSpywareMaster".

The Trojan scans the computer and reports malware in files that are in reality clean system components. If the user clicks the "Remove Now" button, they are taken to the registration page in the hope that they will pay to have the nonexistent threats removed.

[Home](#)[Download](#)[Contact](#)[Advisories](#)[Spyware Information](#)[Browse Threats](#)[False Positive](#)[ThreatNet](#)[Listing Criteria](#)[Spyware Resources](#)

## AdvancedCleaner Threat Display



Copyright © 2008 Sunbelt Software. Reproduction in whole or in part without permission is prohibited.



## AdvancedCleaner

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                 | AdvancedCleaner                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Type</b>                 | Misc                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Type Description</b>     | Miscellaneous threats include applications that do not fit into other categories or that fall into multiple categories. Miscellaneous threats typically include some form of potentially objectionable functionality that may pose privacy or security risks to users and their PCs.                                                                                                                                                                                                       |
| <b>Category</b>             | Rogue Security Program                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Category Description</b> | A Rogue Security Program is software that purports to scan and detect malware or other problems on the computer, but which attempts to dupe or badger users into purchasing the program by presenting the user with intrusive, deceptive warnings and/or false, misleading scan results. Rogue Security Programs typically use aggressive, deceptive advertising and may be installed without adequate notice and consent, often through exploits.                                         |
| <b>Level</b>                | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Level Description</b>    | High risks are typically installed without user interaction through security exploits, and can severely compromise system security. Such risks may open illicit network connections, use polymorphic tactics to self-mutate, disable security software, modify system files, and install additional malware. These risks may also collect and transmit personally identifiable information (PII) without your consent and severely degrade the performance and stability of your computer. |
| <b>Advice Type</b>          | Remove                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Date</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Last updated on</b>      | Sep 24 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>File Traces</b>          | %PROGRAM_FILES%\ advancedcleaner free\ inststat.exe<br>%PROGRAM_FILES%\ advancedcleaner free\ uadc.exe<br>%PROGRAM_FILES%\ advancedcleaner free\ uadccw.exe<br>adcfreeinstaller.exe<br>adcfreesetup.exe<br>b.exe<br>c:\ adcfreeinstaller.exe                                                                                                                                                                                                                                               |

**VIPRE™**  
**Download NOW**  
 (12.6 MB)



## System Requirements:

- Internet Explorer 5.5 +
- 400MHZ+ PC
- 256MB+ RAM
- 150MB of hard drive space
- Windows 2000 Pro SP4 Rollup 1
- Windows Server 2008
- Windows XP SP1, SP2, SP3 (Home, Pro, Media Center, Tablet) 32 and 64-bit
- Windows Vista+ (All flavors) 32 and 64-bit
- Supported Email Applications: Outlook 2000+, Outlook Express 5.0+, Windows Mail on Vista, and SMTP and POP3 (Thunderbird, IncrediMail, Eudora, etc.)
- Installation of VIPRE™ is not supported on Windows 95, 98, or ME, Macintosh or Linux



## VIPRE™ is Here!

High performance, next-generation antivirus + antispyware software VIPRE™ combines antivirus, antispyware, anti-rootkit and other technologies into a seamless, tightly-integrated product. Built with next-generation technology, VIPRE™ (Virus Intrusion Protection Remediation Engine) gives you powerful antivirus software and antispyware software that protects you against today's highly complex malware threats including viruses, adware, spyware and rootkits, without hogging your PC resources like many traditional antivirus products. VIPRE™ is also the first consumer security product to introduce the concept of "Home site licensing".



## Latest Spyware Updates

Our current definitions and software updates:

- VIPRE™**  
 Version: Coming Soon  
 Definition: Coming Soon
- VIPRE™ Enterprise**  
 Version: Coming Soon  
 Definition: Coming Soon

• CounterSpy™ Consumer 2.x

Version 2.5.1043  
Definition: 900 10/26/2008

• CounterSpy™ Consumer 1.5.x

Version: 1.5.82  
Definition: 869 8/22/2008

• CounterSpy™ Enterprise 3.x

Version: 2.0.2200  
Agent Version: 2.0.1312  
Definition: 900 10/26/2008

• CounterSpy™ Enterprise 1.5.x

Version: 1.5.268  
Agent Version: 1.8.1172  
Definition: 869 8/22/2008

• Show all Definitions



**Submit a Threat**

Help the community and submit a threat to be reviewed by our experts.

• Submit A Threat



**Automated Malware Sandbox**

Submit a malware sample to our automated sandbox server to see what the malware would do to your computer if it were installed.

• Submit to Sandbox



**Submit a False Positive**

Have you discovered legitimate software components that are detected as spyware by VIPRE™? Please let us know about it.

• Submit a False Positive



**Software Review Request**

Before submitting a request to have software removed from our database, please read the 'Sunbelt Software Review Process' guidelines, which lay out Sunbelt's policies and procedures for performing software reviews and responding to vendor complaints.

• Software Review Request



**Review Process:**

- html
- pdf



Copyright © 2008 - Sunbelt Software. All rights reserved.  
All products mentioned are trademarks or registered trademarks of their respective companies.



Advisories

Spyware Information

Browse Threats

False Positive

ThreatNet

Listing Criteria

Spyware Resources

## DriveCleaner Threat Display

Search

Copyright © 2008 Sunbelt Software. Reproduction in whole or in part without permission is prohibited.



## DriveCleaner

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                 | DriveCleaner                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Type</b>                 | Misc                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Type Description</b>     | Miscellaneous threats include applications that do not fit into other categories or that fall into multiple categories. Miscellaneous threats typically include some form of potentially objectionable functionality that may pose privacy or security risks to users and their PCs.                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Category</b>             | Rogue Security Program                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Category Description</b> | A Rogue Security Program is software that purports to scan and detect malware or other problems on the computer, but which attempts to dupe or badger users into purchasing the program by presenting the user with intrusive, deceptive warnings and/or false, misleading scan results. Rogue Security Programs typically use aggressive, deceptive advertising and may be installed without adequate notice and consent, often through exploits.                                                                                                                                                                                                                   |
| <b>Level</b>                | Elevated                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Level Description</b>    | Elevated risks are typically installed without adequate notice and consent, and may make unwanted changes to your system, such as reconfiguring your browser's homepage and search settings. These risks may install advertising-related add-ons, including toolbars and search bars, or insert advertising-related components into the Winsock Layered Service Provider chain. These new add-ons and components may block or redirect your preferred network connections, and can negatively impact your computer's performance and stability. Elevated risks may also collect, transmit, and share potentially sensitive data without adequate notice and consent. |
| <b>Advice Type</b>          | Remove                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>          | DriveCleaner is a system cleaning program from Winsoftware that gives exaggerated reports of threats to frighten the user into purchasing the software.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Add. Description</b>     | DriveCleaner uses aggressive, deceptive advertising and pop-ups. DriveCleaner is typically installed through dubious means and the user may not know how it arrived on the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Author</b>               | Innovative Marketing / LocusSoftware                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Author URL</b>           | drivecleaner.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Date</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Last updated on</b>      | Oct 18 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>File Traces</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

```
%local_settings%\ temp\ UDC6_0001_D19M2808\ installer.exe
%program_files%\ common files\ DriveCleaner 2006 Free\ udcps.exe
%program_files%\ common files\ DriveCleaner 2006 Free\ udcscr.exe
%PROGRAM_FILES%\ drivecleaner 2006 free\ insthelp.exe
%PROGRAM_FILES%\ drivecleaner 2006 free\ pv.exe
%PROGRAM_FILES%\ drivecleaner 2006 free\ udc2006.exe
%PROGRAM_FILES%\ DriveCleaner 2006 Free\ UDC6cw.exe
%PROGRAM_FILES%\ drivecleaner 2006 free\ udcpchkl.dll
%PROGRAM_FILES%\ drivecleaner 2006 free\ udcshell.dll
%PROGRAM_FILES%\ drivecleaner 2006 free\ updater.exe
%program_files%\ DriveCleaner Free\ InstHelp.exe
%program_files%\ DriveCleaner Free\ pv.exe
%program_files%\ DriveCleaner Free\ UDC.exe
%program_files%\ DriveCleaner Free\ UDCPChk.dll
%PROGRAM_FILES%\ DriveCleaner 2006 Free\ UDC2006.exe
driveclean-upsetupfree_ch.exe
installdrivecleanerstart.exe
installer.exe
```

Attachment C

## VIPRE™

Download NOW

(12.6 MB)



## System Requirements:

- Internet Explorer 5.5 +
- 400MHZ+ PC
- 256MB+ RAM
- 150MB of hard drive space
- Windows 2000 Pro SP4 Rollup 1
- Windows Server 2008
- Windows XP SP1, SP2, SP3 (Home, Pro, Media Center, Tablet) 32 and 64-bit
- Windows Vista+ (All flavors) 32 and 64-bit
- Supported Email Applications: Outlook 2000+, Outlook Express 5.0+, Windows Mail on Vista, and SMTP and POP3 (Thunderbird, IncrediMail, Eudora, etc.)
- Installation of VIPRE™ is not supported on Windows 95, 98, or ME, Macintosh or Linux



## VIPRE™ is Here!

High performance, next-generation antivirus + antispyware software VIPRE™ combines antivirus, antispyware, anti-rootkit and other technologies into a seamless, tightly-integrated product. Built with next-generation technology, VIPRE™ (Virus Intrusion Protection Remediation Engine) gives you powerful antivirus software and antispyware software that protects you against today's highly complex malware threats including viruses, adware, spyware and rootkits, without hogging your PC resources like many traditional antivirus products. VIPRE™ is also the first consumer security product to introduce the concept of "Home site licensing".



## Latest Spyware Updates

Our current definitions and software updates:

## • VIPRE™

|             |             |
|-------------|-------------|
| Version     | Coming Soon |
| Definition: | Coming Soon |

## • VIPRE™ Enterprise

|             |             |
|-------------|-------------|
| Version     | Coming Soon |
| Definition: | Coming Soon |

## • CounterSpy™ Consumer 2.x

InstHelp.exe  
pv.exe  
setupdrivecleanerstart.exe  
UDC.exe  
udc2006.exe  
UDC6\_cw.exe  
UDC6USS17.exe  
UDCPChk.dll

Version: 2.5.1043  
Definition: 900 10/26/2008

• **CounterSpy™ Consumer 1.5.x**

Version: 1.5.82  
Definition: 969 8/22/2008

• **CounterSpy™ Enterprise 3.x**

Version: 2.0.2200  
Agent Version: 2.0.1312  
Definition: 900 10/26/2008

• **CounterSpy™ Enterprise 1.5.x**

Version: 1.5.268  
Agent Version: 1.8.1172  
Definition: 869 8/22/2008

• Show all Definitions



**Submit a Threat**

Help the community and submit a threat to be reviewed by our experts.

- Submit A Threat



**Automated Malware Sandbox**

Submit a malware sample to our automated sandbox server to see what the malware would do to your computer if it were installed.

- Submit to Sandbox



**Submit a False Positive**

Have you discovered legitimate software components that are detected as spyware by VIPRE™? Please let us know about it.

- Submit a False Positive



**Software Review Request**

Before submitting a request to have software removed from our database, please read the Sunbelt Software Review Process' guidelines, which lay out Sunbelt's policies and procedures for performing software reviews and responding to vendor complaints.

- Software Review Request



**Review Process:**

- [html](#)
- [pdf](#)



Copyright © 2008 - Sunbelt Software. All rights reserved.  
All products mentioned are trademarks or registered trademarks of their respective companies.

[Home](#)[Download](#)[Contact](#)[Advisories](#)[Spyware Information](#)[Browse Threats](#)[False Positive](#)[ThreatNet](#)[Listing Criteria](#)[Spyware Resources](#)

## WinAntiSpyware Threat Display

Copyright © 2008 Sunbelt Software. Reproduction in whole or in part without permission is prohibited.



## WinAntiSpyware

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                 | WinAntiSpyware                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Type</b>                 | Misc                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Type Description</b>     | Miscellaneous threats include applications that do not fit into other categories or that fall into multiple categories. Miscellaneous threats typically include some form of potentially objectionable functionality that may pose privacy or security risks to users and their PCs.                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Category</b>             | Rogue Security Program                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Category Description</b> | A Rogue Security Program is software that purports to scan and detect malware or other problems on the computer, but which attempts to dupe or badger users into purchasing the program by presenting the user with intrusive, deceptive warnings and/or false, misleading scan results. Rogue Security Programs typically use aggressive, deceptive advertising and may be installed without adequate notice and consent, often through exploits.                                                                                                                                                                                                                   |
| <b>Level</b>                | Elevated                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Level Description</b>    | Elevated risks are typically installed without adequate notice and consent, and may make unwanted changes to your system, such as reconfiguring your browser's homepage and search settings. These risks may install advertising-related add-ons, including toolbars and search bars, or insert advertising-related components into the Winsock Layered Service Provider chain. These new add-ons and components may block or redirect your preferred network connections, and can negatively impact your computer's performance and stability. Elevated risks may also collect, transmit, and share potentially sensitive data without adequate notice and consent. |
| <b>Advice Type</b>          | Remove                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>          | WinAntiSpyware is a rogue anti-spyware product which pesters users with scareware tactics to purchase the product.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Add. Description</b>     | WinAntiSpyware is a rogue anti-spyware product which pesters users with scareware tactics to purchase the product.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Author</b>               | Winsoftware                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Author URL</b>           | WinAntiSpyware.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Date</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Last updated on</b>      | Oct 11 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>File Traces</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

%LOCAL\_SETTINGS%\ temp\ NI.UWAS6\_0001\_N91M1508\ setup.exe  
%local\_settings%\ temp\ WinAntiSpyware2006Setup.exe  
%LOCAL\_SETTINGS%\ temporary internet files\ content.ie5\ g5arw9mz\ winantispyware2005scanner2222[1].exe  
%program\_files%\ common files\ WinAntiSpyware 2006 Free\ uwasc.exe  
%program\_files%\ common files\ WinAntiSpyware 2006 Free\ uwasers.exe  
%program\_files%\ winantispyware 2005\ shellex.dll  
%program\_files%\ WinAntiSpyware 2006 Free\ AsAgents.dll  
%PROGRAM\_FILES%\ winantispyware 2006 free\ insthelp.exe  
%program\_files%\ WinAntiSpyware 2006 Free\ shellex.dll  
%PROGRAM\_FILES%\ winantispyware 2006 free\ uwascchk.dll  
%program\_files%\ WinAntiSpyware 2006 Free\ uwascw.exe  
%program\_files%\ WinAntiSpyware 2006 Free\ uwascffNT.exe  
%PROGRAM\_FILES%\ winantispyware 2006 free\ was6.exe  
%program\_files%\ winantispyware 2006 scanner\ shellex.dll  
%PROGRAM\_FILES%\ winantispyware 2007\ was7.exe  
%system%\ drivers\ \_wff.sys  
%system%\ drivers\ uwascsd.sys  
%windows%\ downloaded program files\ uwascy\_0001\_n68m1303netinstaller.exe

VIPRE™  
Download NOW  
(12.6 MB)



## System Requirements:

- Internet Explorer 5.5 +
- 400MHZ+ PC
- 256MB+ RAM
- 150MB of hard drive space
- Windows 2000 Pro SP4 Rollup 1
- Windows Server 2008
- Windows XP SP1, SP2, SP3 (Home, Pro, Media Center, Tablet) 32 and 64-bit
- Windows Vista+ (All flavors) 32 and 64-bit
- Supported Email Applications: Outlook 2000+, Outlook Express 5.0+, Windows Mail on Vista, and SMTP and POP3 (Thunderbird, IncrediMail, Eudora, etc.)
- Installation of VIPRE™ is not supported on Windows 95, 98, or ME, Macintosh or Linux



## VIPRE™ is Here!

High performance, next-generation antivirus + antispyware software  
VIPRE™ combines antivirus, antispyware, anti-rootkit and other technologies into a seamless, tightly-integrated product. Built with next-generation technology, VIPRE™ (Virus Intrusion Protection Remediation Engine) gives you powerful antivirus software and antispyware software that protects you against today's highly complex malware threats including viruses, adware, spyware and rootkits, without hogging your PC resources like many traditional antivirus products. VIPRE™ is also the first consumer security product to introduce the concept of "Home site licensing".



## Latest Spyware Updates

Our current definitions and software updates:

- **VIPRE™**  
Version: Coming Soon  
Definition: Coming Soon
- **VIPRE™ Enterprise**  
Version: Coming Soon  
Definition: Coming Soon
- **CounterSpy™ Consumer 2.x**

winantispyware2006freeinstall.exe  
winantispyware2007freeinstall.exe

Version: 2.5.1043  
Definition: 900 10/26/2008

• **CounterSpy™ Consumer 1.5.x**

Version: 1.5.82  
Definition: 869 8/22/2008

• **CounterSpy™ Enterprise 3.x**

Version: 2.0.2200  
Agent Version: 2.0.1312  
Definition: 900 10/26/2008

• **CounterSpy™ Enterprise 1.5.x**

Version: 1.5.268  
Agent Version: 1.8.1172  
Definition: 869 8/22/2008

• Show all Definitions



**Submit a Threat**

Help the community and submit a threat to be reviewed by our experts.

- Submit A Threat



**Automated Malware Sandbox**

Submit a malware sample to our automated sandbox server to see what the malware would do to your computer if it were installed.

- Submit to Sandbox



**Submit a False Positive**

Have you discovered legitimate software components that are detected as spyware by VIPRE™? Please let us know about it.

- Submit a False Positive



**Software Review Request**

Before submitting a request to have software removed from our database, please read the 'Sunbelt Software Review Process' guidelines, which lay out Sunbelt's policies and procedures for performing software reviews and responding to vendor complaints.

- Software Review Request



**Review Process:**

- html
- pdf



Copyright © 2008 - Sunbelt Software. All rights reserved.  
All products mentioned are trademarks or registered trademarks of their respective companies.

Home

Download

Contact



Advisories

Spyware Information

Browse Threats

False Positive

ThreatNet

Listing Criteria

Spyware Resources

## WinFixer Threat Display

Search

Copyright © 2008 Sunbelt Software. Reproduction in whole or in part without permission is prohibited.



## WinFixer

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                 | WinFixer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Type</b>                 | Misc                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Type Description</b>     | Miscellaneous threats include applications that do not fit into other categories or that fall into multiple categories. Miscellaneous threats typically include some form of potentially objectionable functionality that may pose privacy or security risks to users and their PCs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Category</b>             | Rogue Security Program                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Category Description</b> | A Rogue Security Program is software that purports to scan and detect malware or other problems on the computer, but which attempts to dupe or badger users into purchasing the program by presenting the user with intrusive, deceptive warnings and/or false, misleading scan results. Rogue Security Programs typically use aggressive, deceptive advertising and may be installed without adequate notice and consent, often through exploits.                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Level</b>                | Elevated                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Level Description</b>    | Elevated risks are typically installed without adequate notice and consent, and may make unwanted changes to your system, such as reconfiguring your browser's homepage and search settings. These risks may install advertising-related add-ons, including toolbars and search bars, or insert advertising-related components into the Winsock Layered Service Provider chain. These new add-ons and components may block or redirect your preferred network connections, and can negatively impact your computer's performance and stability. Elevated risks may also collect, transmit, and share potentially sensitive data without adequate notice and consent.                                                                                                                                                                             |
| <b>Advice Type</b>          | Remove                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>          | WinFixer is a disabled data repair utility that nags the user to purchase it in order to fix the problems reported in its scan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Add. Description</b>     | WinFixer is typically installed through security exploits and bundled with malware. WinFixer sponsors an affiliate program via <a href="http://www.softwareprofit.com">www.softwareprofit.com</a> . Webmasters participating in the program are paid according to the sales generated from installation. The program will scan the computer and report errors as repairable but does not provide any details to what is at risk. It then recommends repair that requires a purchase to unlock the program. It also sets a registry key to automatically launch the program on startup. The program communicates with a statistic tracking server for the purpose of web site tracking for its affiliate program. WinFixer may be removed by using the Add/Remove Applet in the Windows Control Panel. WinFixer is the same program as ErrorSafe. |
| <b>Author</b>               | WinSoftware, Ltd                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Author URL</b>           | <a href="http://winfixer.com">winfixer.com</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Date</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Last updated on</b>      | Oct 15 2008                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>File Traces</b>          | %DESKTOPDIRECTORY%\uwfx5netinstaller.exe<br>%DESKTOPDIRECTORY%\winfixer2005scannersetup.exe<br>%DESKTOPDIRECTORY%\winfixer2005trialsetup.exe<br>%DESKTOPDIRECTORY%\winfixerscannerinstall.exe<br>%LOCAL_SETTINGS%\temp\winfixer2005scannersetup.exe<br>%LOCAL_SETTINGS%\temp\winfixer2005setup.exe<br>%LOCAL_SETTINGS%\temp\winfixer2006freesetup.exe<br>%PROGRAM_FILES%\common files\winfixer 2005\fcxml.dll<br>%program_files%\common files\winfixer 2006\pcheck.dll<br>%PROGRAM_FILES%\common files\winsoftware\crxml.dll<br>%program_files%\common files\winsoftware\pcheck.dll<br>%PROGRAM_FILES%\uwfx5_0001_n531025netinstaller.exe<br>%PROGRAM_FILES%\winfixer 2005\compclr.dll                                                                                                                                                           |

## VIPRE™

Download NOW

(12.6 MB)



## System Requirements:

- Internet Explorer 5.5 +
- 400MHZ+ PC
- 256MB+ RAM
- 150MB of hard drive space
- Windows 2000 Pro SP4 Rollup 1
- Windows Server 2008
- Windows XP SP1, SP2, SP3 (Home, Pro, Media Center, Tablet) 32 and 64-bit
- Windows Vista+ (All flavors) 32 and 64-bit
- Supported Email Applications: Outlook 2000+, Outlook Express 5.0+, Windows Mail on Vista, and SMTP and POP3 (Thunderbird, IncrediMail, Eudora, etc.)
- Installation of VIPRE™ is not supported on Windows 95, 98, or ME, Macintosh or Linux



## VIPRE™ is Here!

High performance, next-generation antivirus + antispyware software VIPRE™ combines antivirus, antispyware, anti-rootkit and other technologies into a seamless, tightly-integrated product. Built with next-generation technology, VIPRE™ (Virus Intrusion Protection Remediation Engine) gives you powerful antivirus software and antispyware software that protects you against today's highly complex malware threats including viruses, adware, spyware and rootkits, without hogging your PC resources like many traditional antivirus products. VIPRE™ is also the first consumer security product to introduce the concept of "Home site licensing".



## Latest Spyware Updates

Our current definitions and software updates:

## • VIPRE™

|             |             |
|-------------|-------------|
| Version     | Coming Soon |
| Definition: | Coming Soon |

## • VIPRE™ Enterprise

|             |             |
|-------------|-------------|
| Version     | Coming Soon |
| Definition: | Coming Soon |

erSpy™ Consumer 2.x

Attachment C

Page 188

%PROGRAM\_FILES%\ winfixer 2005\ ffwrpr.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ flfxr\_3.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ ftr.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ fxcrr.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ idletrc.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ mfix.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ str.exe  
 %PROGRAM\_FILES%\ winfixer 2005\ strsr.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ updater.exe  
 %PROGRAM\_FILES%\ winfixer 2005\ uwfx5.exe  
 %PROGRAM\_FILES%\ winfixer 2005\ compcn.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ df\_fixer.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ df\_kmd.sys  
 %PROGRAM\_FILES%\ winfixer 2005\ df\_proxy.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ fcom.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ fwraper.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ filetyperecognizer.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ fixcore.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ install.exe  
 %PROGRAM\_FILES%\ winfixer 2005\ mmfix.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ oedrop.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ sr.exe  
 %PROGRAM\_FILES%\ winfixer 2005\ strsr.dll  
 %PROGRAM\_FILES%\ winfixer 2005\ updater.exe  
 %PROGRAM\_FILES%\ winfixer 2005\ wfx5.exe  
 %PROGRAM\_FILES%\ winfixerfree\ flfxr21.dll  
 %PROGRAM\_FILES%\ winfixerfree\ fwraper.dll  
 %PROGRAM\_FILES%\ winfixerfree\ fxcrr.dll  
 %PROGRAM\_FILES%\ winfixerfree\ insthelp.exe  
 %PROGRAM\_FILES%\ winfixerfree\ mmfix.dll  
 %PROGRAM\_FILES%\ winfixerfree\ updater.exe  
 %PROGRAM\_FILES%\ winfixerfree\ uwfx6.exe  
 %PROGRAM\_FILES%\ winfixerfree\ wfxcheck.dll  
 %SYSTEM%\ df\_kme.exe  
 %SYSTEM%\ dfe1.exe  
 %SYSTEM%\ drivers\ dfdr.sys  
 %windows%\ downloaded program files\  
 uwfx5\_0001\_n66m1101netinstaller.exe  
 ~DC6ScannerSetup.exe  
 1fdb7f6a28d46b0e595fc553b239e6e.exe  
 7bf64a4e562cf5ba809115430d2867a.exe  
 amp1065.exe  
 antivir.exe  
 efcabb.exe  
 ermmcmfe.exe  
 IEFWBHO.dll  
 install\_en.exe  
 installer\_en.exe  
 kpknodnc.exe  
 mmcode003.exe  
 oqatyqba.exe  
 prprotect.exe  
 setup.exe  
 setup\_en.exe  
 setup\_sbd\_en.exe  
 SystemDoctor2006FreeInstall\_it[1].exe  
 uers\_0001\_n68m1801netinstaller.exe  
 uwas5lp\_0001\_0811netinstaller.exe  
 uwfx5\_0001\_lp1014netinstaller.exe  
 uwfx5\_0001\_lpnnetinstaller.exe  
 uwfx5\_0001\_mnnetinstaller.exe  
 uwfx5\_0001\_n57m2112netinstaller.exe  
 uwfx5lp\_0001\_0721netinstaller.exe

Version 2.5.1043  
Definition: 900 10/26/2008

• **CounterSpy™ Consumer 1.5.x**

Version: 1.5.82  
Definition: 869 8/22/2008

• **CounterSpy™ Enterprise 3.x**

Version: 2.0.2200  
Agent Version: 2.0.1312  
Definition: 900 10/26/2008

• **CounterSpy™ Enterprise 1.5.x**

Version: 1.5.268  
Agent Version: 1.8.1172  
Definition: 869 8/22/2008

• Show all Definitions



**Submit a Threat**

Help the community and submit a threat to be reviewed by our experts.

• Submit A Threat



**Automated Malware Sandbox**

Submit a malware sample to our automated sandbox server to see what the malware would do to your computer if it were installed.

• Submit to Sandbox



**Submit a False Positive**

Have you discovered legitimate software components that are detected as spyware by VIPRE™? Please let us know about it.

• Submit a False Positive



**Software Review Request**

Before submitting a request to have software removed from our database, please read the Sunbelt Software Review Process' guidelines, which lay out Sunbelt's policies and procedures for performing software reviews and responding to vendor complaints.

• Software Review Request



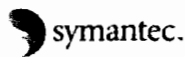
**Review Process:**

- html
- pdf

uwfx5netinstaller.exe  
uwfx5t\_0001\_ipnetinstaller.exe  
uwfx5netinstaller.exe  
uwfx5u\_0001\_ipnetinstaller.exe  
uwfx5netinstaller.exe  
uwfx5vnetinstaller.exe  
uwfx5y\_0001\_n56m1811netinstaller.exe  
uwfx6\_0001\_n69m1503netinstaller.exe  
was5scan[1].exe  
wfi[1].exe  
wshell.dll  
wfxscan[1].exe  
winfixer2005freeinstall.exe  
winfixer2005install[1].exe  
winfixer2005scannerinstall.exe  
winfixer2005scannerinstall[1].exe  
winfixer2005scannerinstall\_es.exe  
winfixer2005scannerinstallde.exe  
winfixer2005scannerinstallfra[1].exe  
winfixer2006freeinstall.exe  
winfixersscannerinstall.exe  
XmlReplacer.exe



Copyright © 2008 - Sunbelt Software. All rights reserved.  
All products mentioned are trademarks or registered trademarks of their respective companies.



## Symantec Security Response

[http://www.symantec.com/security\\_response/index.jsp](http://www.symantec.com/security_response/index.jsp)

# AdvancedCleaner

Updated: July 31, 2007 6:04:47 PM

Type: Misleading Application

Name: AdvancedCleaner

Version: 1.0.35.0

Publisher: AdvancedCleaner

Risk Impact: Medium

Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP

## SUMMARY

### Behavior

AdvancedCleaner is a misleading application, which gives exaggerated reports of security and privacy risks on a computer. The program then prompts the user to purchase a registered version of the software in order to remove the reported risks.

### Protection

Initial Rapid Release version pending

Latest Rapid Release version July 14, 2008 revision 032

Initial Daily Certified version July 31, 2007 revision 016

Latest Daily Certified version August 2, 2008 revision 002

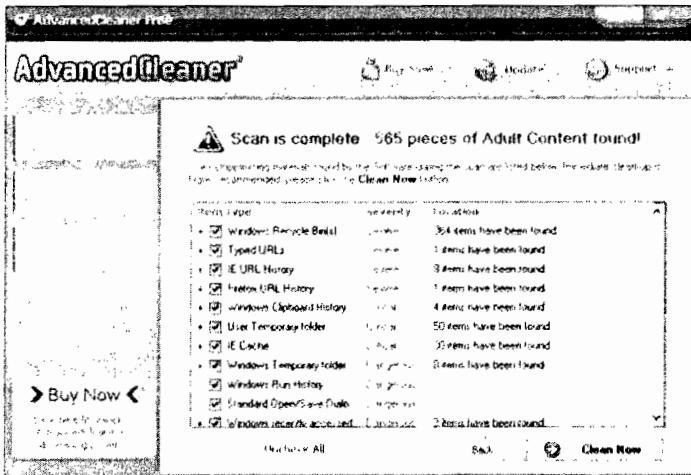
Initial Weekly Certified release date August 1, 2007

[Click here](#) for a more detailed description of Rapid Release and Daily Certified virus definitions.

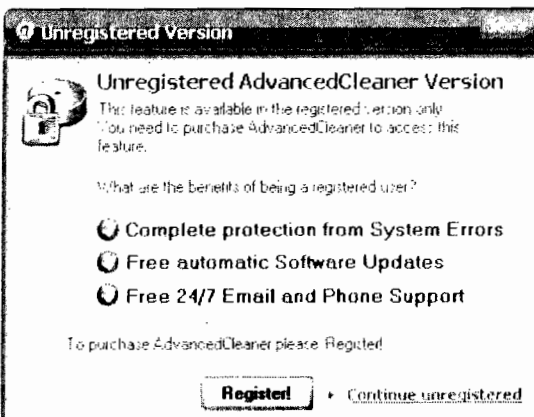
## TECHNICAL DETAILS

### Behavior

When the program is run, it displays a window that allows the user to scan the computer for security threats. The program then reports a number of false threats:



The user is then prompted to pay for a full license of the application in order to remove the falsely reported threats:



The misleading application can be manually downloaded and installed.

#### Installation

When the program is executed, it creates the following files:

```
%UserProfile%\Desktop\AdvancedCleaner Free.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\AdvancedCleaner Free\AdvancedCleaner HomePage.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\AdvancedCleaner Free\AdvancedCleaner Online Manual.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\AdvancedCleaner Free\AdvancedCleaner Online Support.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\AdvancedCleaner Free\Uninstall AdvancedCleaner.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\AdvancedCleaner Free\AdvancedCleaner.lnk
%ProgramFiles%\AdvancedCleaner Free\InstStat.exe
%ProgramFiles%\AdvancedCleaner Free\UADC.exe
%ProgramFiles%\AdvancedCleaner Free\UADCcw.exe
%ProgramFiles%\AdvancedCleaner Free\acu.dat
%ProgramFiles%\AdvancedCleaner Free\antiVlog.dat
%ProgramFiles%\AdvancedCleaner Free\appAct.dat
%ProgramFiles%\AdvancedCleaner Free\AppDB\AppBase.xml
%ProgramFiles%\AdvancedCleaner Free\AppDB\profiles.dat
%ProgramFiles%\AdvancedCleaner Free\AppDB\prowords.dat
%ProgramFiles%\AdvancedCleaner Free\appv.dat
%ProgramFiles%\AdvancedCleaner Free\atl71.dll
%ProgramFiles%\AdvancedCleaner Free\img\button.gif
%ProgramFiles%\AdvancedCleaner Free\img\button2.gif
%ProgramFiles%\AdvancedCleaner Free\img\header.gif
%ProgramFiles%\AdvancedCleaner Free\img\logo.gif
%ProgramFiles%\AdvancedCleaner Free\img\spacer.gif
%ProgramFiles%\AdvancedCleaner Free\img\top1.jpg
%ProgramFiles%\AdvancedCleaner Free\img\top2.jpg
%ProgramFiles%\AdvancedCleaner Free\img\top_line.gif
%ProgramFiles%\AdvancedCleaner Free\lapv.dat
%ProgramFiles%\AdvancedCleaner Free\license.rtf
%ProgramFiles%\AdvancedCleaner Free\manual.url
%ProgramFiles%\AdvancedCleaner Free\mf71.dll
%ProgramFiles%\AdvancedCleaner Free\msvcp71.dll
%ProgramFiles%\AdvancedCleaner Free\msvc71.dll
%ProgramFiles%\AdvancedCleaner Free\naglinks.dat
%ProgramFiles%\AdvancedCleaner Free\readme.rtf
%ProgramFiles%\AdvancedCleaner Free\report.dat
%ProgramFiles%\AdvancedCleaner Free\req.dat
%ProgramFiles%\AdvancedCleaner Free\request.dat
%ProgramFiles%\AdvancedCleaner Free\support.url
%ProgramFiles%\AdvancedCleaner Free\tasks.dat
%ProgramFiles%\AdvancedCleaner Free\transformer.dat
%ProgramFiles%\AdvancedCleaner Free\UADC.url
%ProgramFiles%\AdvancedCleaner Free\UADC.xml
%ProgramFiles%\AdvancedCleaner Free\unins000.dat
%ProgramFiles%\AdvancedCleaner Free\unins000.exe
%ProgramFiles%\AdvancedCleaner Free\uninstall.ico
%ProgramFiles%\AdvancedCleaner Free\UninstallPage.html
%ProgramFiles%\AdvancedCleaner Free\upser.dat
%UserProfile%\Local Settings\Temp\UADC_0001_[EIGHT RANDOM CHARACTERS]\installer.exe
```

Next, the program creates the following registry entries so that it executes whenever Windows starts:

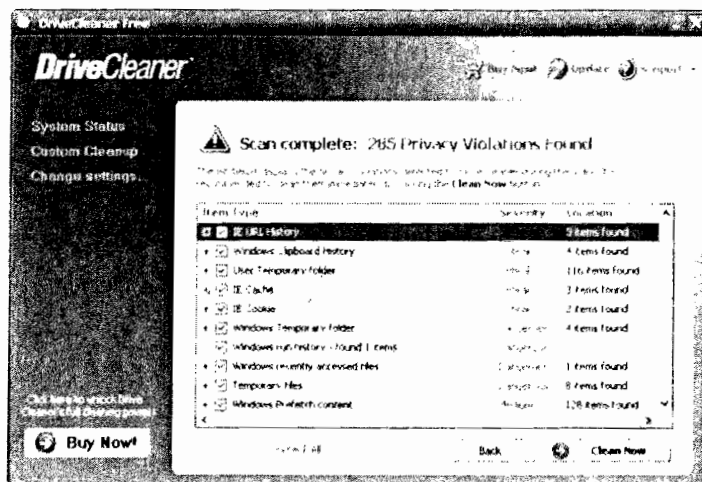
```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AdvancedCleaner Free = "C:\Program Files\AdvancedCleaner Free\UADC.exe" /min
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\UADC_104911963 = "C:\Program Files\AdvancedCleaner Free\UADCcw.exe" -c"
```

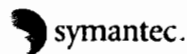
It also creates the following registry subkeys:

```
HKEY_ALL_USERS\Software\AdvancedCleaner Free
HKEY_LOCAL_MACHINE\SOFTWARE\AdvancedCleaner Free
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\UADC_is1
HKEY_LOCAL_MACHINE\SOFTWARE\UADC_[EIGHT RANDOM CHARACTERS]
```

#### Similar Security Risks

DriveCleaner



**Symantec Security Response**

[http://www.symantec.com/security\\_response/index.jsp](http://www.symantec.com/security_response/index.jsp)

**WinFixer**

**Updated:** June 22, 2007 1:14:40 PM

**Type:** Misleading Application

**Name:** WinAntivirusPro: Amaena

**Version:** WinFixer 2005 1.0

**Publisher:** WinSoftware Ltd

**Risk Impact:** Medium

**Systems Affected:** Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

**SUMMARY****Behavior**

WinFixer is a Security Risk that may give exaggerated reports of threats on the computer. The program then prompts the user to purchase a registered version of the software in order to remove the reported threats.

**Protection**

**Initial Rapid Release version** June 27, 2007

**Latest Rapid Release version** October 9, 2008 revision 053

**Initial Daily Certified version** June 27, 2007

**Latest Daily Certified version** October 9, 2008 revision 054

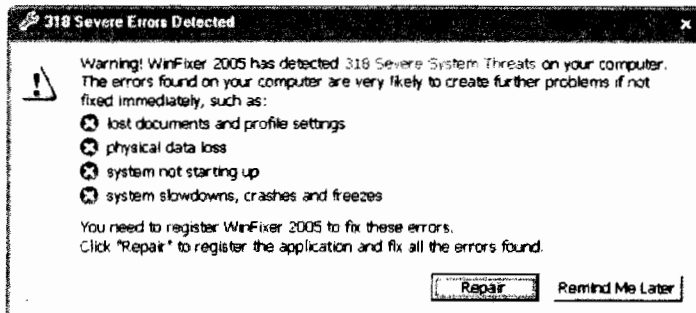
**Initial Weekly Certified release date** December 7, 2005

[Click here](#) for a more detailed description of Rapid Release and Daily Certified virus definitions.

**TECHNICAL DETAILS****Behaviour**

This misleading application can be manually downloaded and installed.

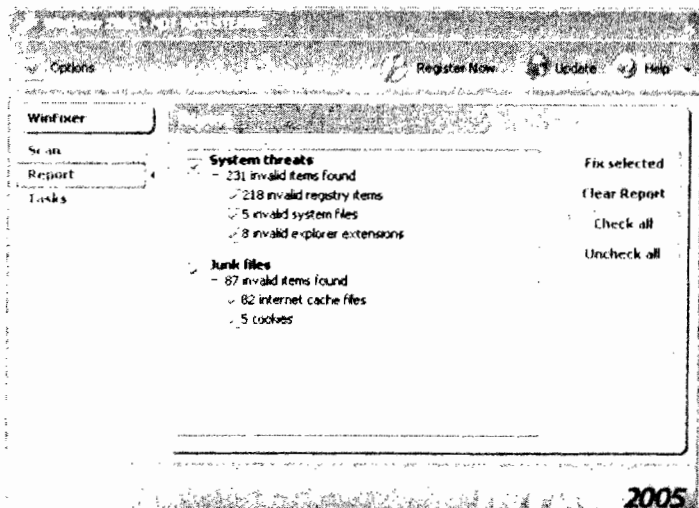
The program falsely reports a number of infected objects on the computer.



The program reports the following items as System threats:

Invalid explorer extensions

Invalid system files



It then prompts the user to purchase a registered version of the software in order to remove the reported threats.

#### Installation

When WinFixer is executed, it creates the following files.

C:\Documents and Settings\administrator\Desktop\WinFixer 2005.lnk  
 C:\Documents and Settings\administrator\Local Settings\Temp\WinFixer2005ScannerSetup.exe  
 C:\Documents and Settings\All Users\Start Menu\Programs\WinFixer 2005\Contact customer support.lnk  
 C:\Documents and Settings\All Users\Start Menu\Programs\WinFixer 2005\Uninstall WinFixer 2005.lnk  
 C:\Documents and Settings\All Users\Start Menu\Programs\WinFixer 2005\WinFixer 2005 on the Web.lnk  
 C:\Documents and Settings\All Users\Start Menu\Programs\WinFixer 2005\WinFixer 2005.lnk  
 %ProgramFiles%\Common Files\WinSoftware\CrXML.dll  
 %ProgramFiles%\Common Files\WinSoftware\PCCheck.dll  
 %ProgramFiles%\WinFixer 2005\Activate.dat  
 %ProgramFiles%\WinFixer 2005\bnlink.dat  
 %ProgramFiles%\WinFixer 2005\compcln.dll  
 %ProgramFiles%\WinFixer 2005\DataBase.sav  
 %ProgramFiles%\WinFixer 2005\df\_fixer.dll  
 %ProgramFiles%\WinFixer 2005\df\_kmd.sys  
 %ProgramFiles%\WinFixer 2005\df\_proxy.dll  
 %ProgramFiles%\WinFixer 2005\ffCom.dll  
 %ProgramFiles%\WinFixer 2005\FFWrapper.dll  
 %ProgramFiles%\WinFixer 2005\FileTypeRecognizer.dll  
 %ProgramFiles%\WinFixer 2005\FixCore.dll  
 %ProgramFiles%\WinFixer 2005\flash.ini  
 %ProgramFiles%\WinFixer 2005\Install.exe  
 %ProgramFiles%\WinFixer 2005\lapv.dat  
 %ProgramFiles%\WinFixer 2005\License.rtf  
 %ProgramFiles%\WinFixer 2005\lock.dat  
 %ProgramFiles%\WinFixer 2005\MMFix.dll  
 %ProgramFiles%\WinFixer 2005\OEDrop.dll  
 %ProgramFiles%\WinFixer 2005\Program.sav  
 %ProgramFiles%\WinFixer 2005\pv.dat  
 %ProgramFiles%\WinFixer 2005\sr.exe  
 %ProgramFiles%\WinFixer 2005\sr.log  
 %ProgramFiles%\WinFixer 2005\StrRes.dll  
 %ProgramFiles%\WinFixer 2005\support.url  
 %ProgramFiles%\WinFixer 2005\Template.dbx  
 %ProgramFiles%\WinFixer 2005\trace.log  
 %ProgramFiles%\WinFixer 2005\unins000.dat  
 %ProgramFiles%\WinFixer 2005\unins000.exe  
 %ProgramFiles%\WinFixer 2005\up.dat  
 %ProgramFiles%\WinFixer 2005\update.log  
 %ProgramFiles%\WinFixer 2005\updater.dat  
 %ProgramFiles%\WinFixer 2005\Updater.exe  
 %ProgramFiles%\WinFixer 2005\WFX5.exe  
 %ProgramFiles%\WinFixer 2005\wfx5.url  
 %System%\drivers\df\_kmd.sys  
 %System%\system32\df\_kme.exe

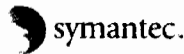
Next, the program creates the following registry entry so that it executes whenever Windows starts:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WinFixer 2005 = "C:\Program Files\WinFixer 2005\WFX5.exe"

The program then creates the following registry subkeys:

HKEY\_CLASSES\_ROOT\AppID\CheckProduct2.DLL  
 HKEY\_CLASSES\_ROOT\AppID\compcln.dll  
 HKEY\_CLASSES\_ROOT\AppID\FFWrapper.DLL  
 HKEY\_CLASSES\_ROOT\AppID\FixCore.DLL  
 HKEY\_CLASSES\_ROOT\AppID\MMFix.Ctrl.DLL  
 HKEY\_CLASSES\_ROOT\AppID\{25A3C995-10C8-474B-A167-99460AB4AB2B}  
 HKEY\_CLASSES\_ROOT\AppID\{287A2BAD-6590-4EFF-9BBC-494385664A73}  
 HKEY\_CLASSES\_ROOT\AppID\{290B5B73-4963-4BA1-9D2D-07CB566CB7FA}  
 HKEY\_CLASSES\_ROOT\AppID\{8C65AEF6-E413-4314-815B-82717A3F1603}  
 HKEY\_CLASSES\_ROOT\AppID\{E8928E69-C050-42A9-8884-94DE85E888A2}  
 HKEY\_CLASSES\_ROOT\CLSID\{08C71FB1-1E66-4D22-9F32-4C045A451306}  
 HKEY\_CLASSES\_ROOT\CLSID\{1CDEB41B-905A-4183-AA20-26E075419B46}  
 HKEY\_CLASSES\_ROOT\CLSID\{38EDB9E2-D7C4-4575-8905-FE65414FFEAD}  
 HKEY\_CLASSES\_ROOT\CLSID\{48349992-1402-4C67-B45B-2E619E641FDB}  
 HKEY\_CLASSES\_ROOT\CLSID\{538BC8F3-2E1E-4D2D-A261-158DF6E9B407}  
 HKEY\_CLASSES\_ROOT\CLSID\{53ABACCB-434C-4756-A02B-8C2A3F29FB7D}  
 HKEY\_CLASSES\_ROOT\CLSID\{66A9C4D0-BC54-4841-8FAA-DB98CBB77BAD}  
 HKEY\_CLASSES\_ROOT\CLSID\{84C43108-013C-4513-8578-F50080B9C9D0}  
 HKEY\_CLASSES\_ROOT\CLSID\{9CC1BE04-3B42-4442-9A46-77E8BC1108F9}  
 HKEY\_CLASSES\_ROOT\CLSID\{AA69BBFC-1D28-4960-8061-93C1BB156238}  
 HKEY\_CLASSES\_ROOT\CLSID\{B096A483-0ABD-4AF0-856A-CAD36145AF5C}  
 HKEY\_CLASSES\_ROOT\CLSID\{B5E427F9-AB38-4348-9076-86870C2BE860}  
 HKEY\_CLASSES\_ROOT\CLSID\{C0BC364F-AB33-4778-8047-5A2148E0ECDA}

HKEY\_CLASSES\_ROOT\CLSID\{CAE8A9B1-ABBD-4159-A485-1DA045A5D4A1}  
HKEY\_CLASSES\_ROOT\CLSID\{F41C1430-CFDE-4AD3-B38D-7890F0843E47}  
HKEY\_CLASSES\_ROOT\Interface\{08C71FB1-1E66-4D22-9F32-4C045A451306}  
HKEY\_CLASSES\_ROOT\Interface\{1CE1C25B-F8B4-4974-99D2-5D4AE96B9900}  
HKEY\_CLASSES\_ROOT\Interface\{35096C29-3507-4ABE-B6D8-C7CC881BE020}  
HKEY\_CLASSES\_ROOT\Interface\{38F743A2-210F-49DE-9B79-DCD501CED284}  
HKEY\_CLASSES\_ROOT\Interface\{3EEC290D-FC13-4C83-803D-4802651EEB61}  
HKEY\_CLASSES\_ROOT\Interface\{41A5BBF6-3C9D-4CF9-9A99-32DD37CC290B}  
HKEY\_CLASSES\_ROOT\Interface\{4E4F38D9-8736-41AE-B192-E829AE194398}  
HKEY\_CLASSES\_ROOT\Interface\{4F79D1C5-24F9-4E59-8022-604D4B41D5CA}  
HKEY\_CLASSES\_ROOT\Interface\{66484903-09F4-4330-927D-1F6C214221AC}  
HKEY\_CLASSES\_ROOT\Interface\{7FA14AD6-D8E5-465F-9BD1-A37E26C1A74F}  
HKEY\_CLASSES\_ROOT\Interface\{9E984934-CD94-4763-9DBC-618E483D4B7F}  
HKEY\_CLASSES\_ROOT\Interface\{B115BD8E-B008-46F4-B8B6-3405EB325C3C}  
HKEY\_CLASSES\_ROOT\Interface\{B9DFCF32-B679-4CAD-B7FC-518A48CE3922}  
HKEY\_CLASSES\_ROOT\Interface\{CAE8A9B1-ABBD-4159-A485-1DA045A5D4A1}  
HKEY\_CLASSES\_ROOT\Interface\{CBEEF194-EBC5-4758-9B51-AC34FC135E70}  
HKEY\_CLASSES\_ROOT\Interface\{CD3604CC-2B95-43EE-AFC9-E7444C21BE1C}  
HKEY\_CLASSES\_ROOT\Interface\{D21040FE-0A57-4FAB-8ED2-F0E653E55809}  
HKEY\_CLASSES\_ROOT\Interface\{D7A2488E-53E4-4EDD-AEAA-F24778BEB100}  
HKEY\_CLASSES\_ROOT\Interface\{D7A6DF8D-B6CF-4C27-8E99-ECA2CE370EA7}  
HKEY\_CLASSES\_ROOT\Interface\{F41C1430-CFDE-4AD3-B38D-7890F0843E47}  
HKEY\_CLASSES\_ROOT\Interface\{F6C1582E-B11C-4724-B8F6-240457EF1D2A}  
HKEY\_CLASSES\_ROOT\Interface\{FB787D5E-0C7C-4BAB-B45D-20325FB886DB}  
HKEY\_CLASSES\_ROOT\TypeLib\{0E9F6AC0-A21A-4591-910F-E2C6F3CA094C}  
HKEY\_CLASSES\_ROOT\TypeLib\{30ED49A5-CA6C-4918-B5F3-5E6818C91D8B}  
HKEY\_CLASSES\_ROOT\TypeLib\{4DCEEA42-794D-4855-9ECC-20DC5F4FEA7}  
HKEY\_CLASSES\_ROOT\TypeLib\{6A077841-5016-42C8-92C8-F2D6B865BCD1}  
HKEY\_CLASSES\_ROOT\TypeLib\{AD70AC89-F460-4E7E-B5A5-7EAF7E207736}  
HKEY\_CLASSES\_ROOT\TypeLib\{B6625280-8CD8-4632-97C0-83CEC12A49A3}  
HKEY\_CLASSES\_ROOT\TypeLib\{F458ADAE-D53B-4859-B99F-9FA127791278}  
HKEY\_CLASSES\_ROOT\TypeLib\{FC76A5B8-DB35-4F3E-8B9A-BF0EEA098D64}  
HKEY\_CLASSES\_ROOT\CheckProduct2.CheckProduct.1  
HKEY\_CLASSES\_ROOT\CompCleanCore.AppCleaner  
HKEY\_CLASSES\_ROOT\CompCleanCore.AppCleaner.1  
HKEY\_CLASSES\_ROOT\CompCleanCore.CCQuickScan  
HKEY\_CLASSES\_ROOT\CompCleanCore.CCQuickScan.1  
HKEY\_CLASSES\_ROOT\CompCleanCore.FileCleaner  
HKEY\_CLASSES\_ROOT\CompCleanCore.FileCleaner.1  
HKEY\_CLASSES\_ROOT\CompCleanCore.InetCleaner  
HKEY\_CLASSES\_ROOT\CompCleanCore.InetCleaner.1  
HKEY\_CLASSES\_ROOT\CompCleanCore.RegCleaner  
HKEY\_CLASSES\_ROOT\CompCleanCore.RegCleaner.1  
HKEY\_CLASSES\_ROOT\CompCleanCore.SystemCleaner  
HKEY\_CLASSES\_ROOT\CompCleanCore.SystemCleaner.1  
HKEY\_CLASSES\_ROOT\df\_fixer.Fixer  
HKEY\_CLASSES\_ROOT\df\_fixer.Fixer.1  
HKEY\_CLASSES\_ROOT\df\_proxy.DriverManipulate  
HKEY\_CLASSES\_ROOT\df\_proxy.DriverManipulate.1  
HKEY\_CLASSES\_ROOT\FFCom.FIFixer  
HKEY\_CLASSES\_ROOT\FFWrapper.FFEngineWrapper  
HKEY\_CLASSES\_ROOT\FFWrapper.FFEngineWrapper.1  
HKEY\_CLASSES\_ROOT\FixCore.MMFixCore  
HKEY\_CLASSES\_ROOT\FixCore.MMFixCore.1  
HKEY\_CLASSES\_ROOT\MMFixCtrl.CoFixEngine  
HKEY\_CLASSES\_ROOT\MMFixCtrl.CoFixEngine.1  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WFX5\_is1  
HKEY\_LOCAL\_MACHINE\SOFTWARE\WinSoftware\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet  
Control\SafeBoot\Minimal\df\_km.sys  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\df\_kmd.sys  
HKEY\_CURRENT\_USER\Software\WinSoftware

**Symantec Security Response**

[http://www.symantec.com/security\\_response/index.jsp](http://www.symantec.com/security_response/index.jsp)

**WinAntiSpyware**

**Updated:** February 13, 2007 11:48:42 AM

**Type:** Misleading Application

**Version:** 3.0.28.4

**Publisher:** WinAntiSpyware

**Risk Impact:** Medium

**File Names:** uwas6chk.dll uwasffNT.exe was6.exe WAS6.url uwasfsd.sys wasfsd.sys ApiMon.sys was6chk.dll

**Systems Affected:** Windows 2000, Windows 98, Windows NT, Windows XP

**SUMMARY****Behavior**

WinAntiSpyware is a potentially unwanted application that may use aggressive marketing techniques. There may be a number of versions from the same vendor that may vary in behaviour.

**Symptoms**

Your Symantec program detects WinAntiSpyware.

**Transmission**

This security risk is manually downloaded and installed.

**Protection**

**Initial Rapid Release version** March 7, 2006

**Latest Rapid Release version** October 8, 2008 revision 020

**Initial Daily Certified version** March 7, 2006

**Latest Daily Certified version** October 8, 2008 revision 023

**Initial Weekly Certified release date** March 8, 2006

[Click here](#) for a more detailed description of Rapid Release and Daily Certified virus definitions.

**TECHNICAL DETAILS**

When WinAntiSpyware is executed, it performs the following actions:

Creates the following files:

C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006 Scanner  
Contact customer support.lnk  
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006 Scanner  
Uninstall WinAntiSpyware 2006 Scanner.lnk  
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006 Scanner  
WinAntiSpyware 2006 Scanner on the Web.lnk  
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006 Scanner  
WinAntiSpyware 2006 Scanner Online Manual.lnk  
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006 Scanner  
WinAntiSpyware 2006 Scanner.lnk  
%UserProfile%\application data\microsoft\internet explorer\quick launch\WinAntispyware 2006.lnk  
%UserProfile%\Desktop\WinAntiSpyware 2006 Scanner.lnk  
%UserProfile%\Local Settings\Temp\WinAntiSpyware2006Setup.exe  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\Activate.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\AsAgents.dll  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\bnlink.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\appupdate.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\AutoProcess.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\dbupdate.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\enemies.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\knownfiles.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\monstate.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\PortSpec.ats  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\quarantine.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\RTMonitor.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\Summary.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\tasks.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\database\TEBase.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\InstHelp.exe  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\lapv.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\license.rtf  
%ProgramFiles%\WinAntiSpyware 2006 Scanner>manual.url  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\pv.dat  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\shellex.dll  
%ProgramFiles%\WinAntiSpyware 2006 Scanner\log

```
%ProgramFiles%\WinAntiSpyware 2006 Scanner\unins000.dat
%ProgramFiles%\WinAntiSpyware 2006 Scanner\unins000.exe
%ProgramFiles%\WinAntiSpyware 2006 Scanner\updater.dat
%ProgramFiles%\WinAntiSpyware 2006 Scanner\Updater.exe
%ProgramFiles%\WinAntiSpyware 2006 Scanner\was6chk.dll
%ProgramFiles%\WinAntiSpyware 2006 Scanner\was6ffNT.exe
%ProgramFiles%\WinAntiSpyware 2006 Scanner\vbvpv.dat
%ProgramFiles%\WinAntiSpyware 2006 Scanner\was6.exe
%ProgramFiles%\WinAntiSpyware 2006 Scanner\WAS6.url
%CommonProgramFiles%\WinAntiSpyware 2006\was6chk.dll
%ProgramFiles%\WinAntiSpyware 2006\Activate.dat
%ProgramFiles%\WinAntiSpyware 2006\AsAgents.dll
%ProgramFiles%\WinAntiSpyware 2006\AsAgents.xml
%ProgramFiles%\WinAntiSpyware 2006\database\enemies.dat
%ProgramFiles%\WinAntiSpyware 2006\database\knownfiles.dat
%ProgramFiles%\WinAntiSpyware 2006\database\TEBase.dat
%ProgramFiles%\WinAntiSpyware 2006\InstHelp.exe
%ProgramFiles%\WinAntiSpyware 2006\lapv.dat
%ProgramFiles%\WinAntiSpyware 2006\license.rtf
%ProgramFiles%\WinAntiSpyware 2006\manual.pdf
%ProgramFiles%\WinAntiSpyware 2006\ps.dat
%ProgramFiles%\WinAntiSpyware 2006\pv.dat
%ProgramFiles%\WinAntiSpyware 2006\shellex.xml
%ProgramFiles%\WinAntiSpyware 2006\shellex.dll
%ProgramFiles%\WinAntiSpyware 2006\support.exe
%ProgramFiles%\WinAntiSpyware 2006\threatnet.ini
%ProgramFiles%\WinAntiSpyware 2006\unins000.dat
%ProgramFiles%\WinAntiSpyware 2006\unins000.exe
%ProgramFiles%\WinAntiSpyware 2006\UnWizard.exe
%ProgramFiles%\WinAntiSpyware 2006\unwizard.xml
%ProgramFiles%\WinAntiSpyware 2006\updater.dat
%ProgramFiles%\WinAntiSpyware 2006\vbvpv.dat
%ProgramFiles%\WinAntiSpyware 2006\was6.exe
%ProgramFiles%\WinAntiSpyware 2006\WAS6.url
%ProgramFiles%\WinAntiSpyware 2006\WAS6.xml
%ProgramFiles%\WinAntiSpyware 2006\was6ffNT.exe
%System%\drivers\was6sd.sys
%System%\drivers\ApMon.sys
%System%\drivers\was6sd.sys
%System%\stera.exe
%System%\ati71.dll
%System%\mfc71.dll
%Windir%\is-[RANDOM].exe
%Windir%\is-[RANDOM].lst
%Windir%\is-[RANDOM].msg
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer
\Quick Launch\WinAntiSpyware 2006.lnk
C:\Documents and Settings\Administrator\Desktop\WinAntiSpyware 2006.lnk
C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft
\Media Player\wmpfolders.wmdb
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006\Feedback on Support Quality.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006\Report Software Defect.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006\Request for Instructions.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006\Share Your Suggestions.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006\Uninstall WinAntiSpyware 2006.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006\WinAntiSpyware 2006 Manual.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006\WinAntiSpyware 2006 on the Web.lnk
C:\Documents and Settings\All Users\Start Menu\Programs\WinAntiSpyware 2006\WinAntiSpyware 2006.lnk
```

**Notes:**

%ProgramFiles% is a variable that refers to the program files folder. By default, this is C:\Program Files.

%CommonProgramFiles% is a variable that refers to the Common Files folder. By default, this is C:\Program Files\Common Files.

%System% is a variable that refers to the System folder. By default this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

Creates the following registry subkeys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes*.shellex\ContextMenuHandlers\Explorer\WAS
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0D7DE264-2FDD-4C09-9077-3DC4A2DBE9D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{1200649B-B9B6-44A5-B359-9B09EBEA6311}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{12A6DE55-EDED-4675-AF10-B415EDDB1D7A}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{AEC04567-46B5-4b77-AAC5-396D70923B11}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{CLSID_ShellExecContextMenuHandler}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\shellex\ContextMenuHandlers
\Explorer\WAS
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\ContextMenuHandlers\Explorer\WAS
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{4597AB12-A884-4CA6-B729-CEDE12FEF096}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{AEC04567-AD73-41E9-86E5-53A2F5D93411}
```

Attachment C

Page 198

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{13446771-7344-4064-8000-000000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{406771-7344-4064-8000-000000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{ABCD4567-4D73-43E9-85E5-5A2DBD95422}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WAS6.WAS6
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\wasfsd.CreationNotifier
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\wasfsd.CreationNotifier.1
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\wasshellex.ShellEx
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\wasshellex.ShellEx.1
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\wasshellex.WASContextMenu
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\wasshellex.WASContextMenu.1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\URLSearchHooks
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinAntiSpyware 2006 Scanner.is1
HKEY_LOCAL_MACHINE\SOFTWARE\WinAntiSpyware 2006 Scanner
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\wasfsd
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wasfsd
HKEY_USERS\S-1-5-21-220523388-1844823847-682003330-500\Software\Mirabilis
HKEY_USERS\S-1-5-21-220523388-1844823847-682003330-500\Software\Mirabilis\ICQ
HKEY_USERS\S-1-5-21-220523388-1844823847-682003330-500\Software\Mirabilis\ICQAgent
HKEY_USERS\S-1-5-21-220523388-1844823847-682003330-500\Software\Mirabilis\ICQAgent\Apps
HKEY_USERS\S-1-5-21-220523388-1844823847-682003330-500\Software\WinAntiSpyware 2006 Scanner
HKEY_USERS\S-1-5-21-220523388-1844823847-682003330-500\Software\WinAntiSpyware 2006 Scanner\Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{ABCD4567-76B5-4bc7-AAC5-396D70925B22}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{ABCD4567-4D73-43E9-85E5-5A2DBD95422}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{ABCD4567-7437-43EF-AB74-4AB1D3A37422}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\wasfsd.CreationNotifier
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\wasfsd.CreationNotifier.1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WAS.is1
HKEY_LOCAL_MACHINE\SOFTWARE\WinAntiSpyware 2006
HKEY_ALL_USERS\Software\WinAntiSpyware 2006
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wasfsd
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\{*\shellex\ContextMenuHandlers\Explorer\WAS
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\ContextMenuHandlers\Explorer\WAS
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\shellex\ContextMenuHandlers\Explorer\WAS
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\UWAS6.UWAS6
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\wasshellex.WASContextMenu
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\wasshellex.WASContextMenu.1
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WASPchk.WASPchk
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SYSTEM\ControlSet001\Services\wasfsd
```

Adds the value:

"WinAntispyware 2006 Scanner" = "C:\Program Files\WinAntispyware 2006 Scanner\was6.exe"

to the registry subkeys:

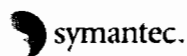
```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
```

so that the risk runs every time Windows starts.

Displays alert messages when changes are made on the compromised computer. The activity in question is halted until the user clicks Allow or five seconds have passed.

The types of activities that the risk blocks include the following:

Changes to the browser's home page  
Installation of software



## Symantec Security Response

[http://www.symantec.com/security\\_response/index.jsp](http://www.symantec.com/security_response/index.jsp)

## ErrorSafe

**Updated:** February 13, 2007 11:47:48 AM

**Type:** Misleading Application

**Infection Length:** 1.8 MB

**Version:** 1.0.46.0

**Publisher:** ErrorSafe Inc.

**Risk Impact:** Medium

**Systems Affected:** Windows 2000, Windows NT, Windows Server 2003, Windows XP

## SUMMARY

### Behavior

ErrorSafe is a Security Risk that may give exaggerated reports of threats on the computer. The program then prompts the user to purchase a registered version of the software in order to remove the reported threats.

### Symptoms

Your Symantec program detects ErrorSafe.

### Transmission

This security risk is manually downloaded and installed.

### Protection

**Initial Rapid Release version** January 21, 2006

**Latest Rapid Release version** June 14, 2008 revision 017

**Initial Daily Certified version** January 21, 2006

**Latest Daily Certified version** August 2, 2008 revision 002

**Initial Weekly Certified release date** January 25, 2006

[Click here](#) for a more detailed description of Rapid Release and Daily Certified virus definitions.

## TECHNICAL DETAILS

When ErrorSafe is executed, it performs the following actions:

Creates some of the following files and folders:

%UserProfile%\Desktop\ErrorSafe.lnk  
 C:\Documents and Settings\All Users\Start Menu\Programs\ErrorSafe\Contact customer support.lnk  
 C:\Documents and Settings\All Users\Start Menu\Programs\ErrorSafe\Uninstall ErrorSafe.lnk  
 C:\Documents and Settings\All Users\Start Menu\Programs\ErrorSafe\ErrorSafe.lnk  
 C:\Documents and Settings\All Users\Start Menu\Programs\ErrorSafe\ErrorSafe on the Web.lnk  
 %ProgramFiles%\ErrorSafe\Backup  
 %ProgramFiles%\ErrorSafe\Mp3DB  
 %ProgramFiles%\ErrorSafe\MpegDB  
 %ProgramFiles%\ErrorSafe\Repaired  
 %ProgramFiles%\ErrorSafe\Tasks  
 %ProgramFiles%\ErrorSafe\WaveDB  
 %ProgramFiles%\ErrorSafe\ERS.EXE  
 %ProgramFiles%\ErrorSafe\Install.exe  
 %ProgramFiles%\ErrorSafe\sr.exe  
 %ProgramFiles%\ErrorSafe\unins000.exe  
 %ProgramFiles%\ErrorSafe\sr.exe  
 %ProgramFiles%\ErrorSafe\sr.log  
 %ProgramFiles%\ErrorSafe\df\_fixer.dll  
 %ProgramFiles%\ErrorSafe\df\_proxy.dll  
 %ProgramFiles%\ErrorSafe\ecc.dll  
 %ProgramFiles%\ErrorSafe\esSPCheck.dll  
 %ProgramFiles%\ErrorSafe\FWWrapper.dll  
 %ProgramFiles%\ErrorSafe\FixCore.dll  
 %ProgramFiles%\ErrorSafe\FiFix5.dll  
 %ProgramFiles%\ErrorSafe\FTRec.dll  
 %ProgramFiles%\ErrorSafe\MMFix.dll  
 %ProgramFiles%\ErrorSafe\StrRes.dll  
 %ProgramFiles%\ErrorSafe\flash.ini  
 %ProgramFiles%\ErrorSafe\Activate.dat  
 %ProgramFiles%\ErrorSafe\btlink.dat  
 %ProgramFiles%\ErrorSafe\lapv.dat  
 %ProgramFiles%\ErrorSafe\lock.dat  
 %ProgramFiles%\ErrorSafe\pv.dat  
 %ProgramFiles%\ErrorSafe\unins000.dat  
 %ProgramFiles%\ErrorSafe\Template.dhx

```
%ProgramFiles%\ErrorSafe\support.rul
%ProgramFiles%\ErrorSafe\License.rtf
%ProgramFiles%\ErrorSafe\DataBase.sav
%ProgramFiles%\ErrorSafe\Program.sav
%ProgramFiles%\ErrorSafe\ersd.sys
%ProgramFiles%\ErrorSafe\erssdd.sys
%ProgramFiles%\ErrorSafe\trace.log
%System%\drivers\ersd.sys
%System%\df_kme.exe
```

**Notes:**

%UserProfile% is a variable that refers to the current user's profile folder. By default, this is C:\Documents and Settings\{CURRENT USER} (Windows NT/2000/XP).

%ProgramFiles% is a variable that refers to the program files folder. By default, this is C:\Program Files.

%System% is a variable that refers to the System folder. By default this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

Creates the following registry subkeys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{0324ED1-05C0-443a-A34F-98BFC64426F5}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID
\1184B0A26-4C9C-4757-ABF5-4B6AF71F9A45}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{18A41B20-E511-47a1-B345-FFC290730E9B}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{259D1063-5414-41b0-86D5-AABB7A5D7DA7}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{2B314C12-40CA-43ef-913A-61A8105C4C0D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{43DB73EB-4C90-4418-B6AD-1CDB22016008}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{4AA76F27-81BC-4C3F-9F24-CB90749C8CC9}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{4F4E2324-42AD-41e4-B9d6-B6D30C7BF90A}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{5234A2A-EF00-4750-9B8C-E5B907D26536}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{54397033-FB54-48AB-8AE4-AE108B36DAB4}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{6AE7418B-129F-4A2C-AE1B-D5962838F02D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{7D435027-F646-4bf9-B2C5-0EF4940D5CA2}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{8DAE9102-0010-4D30-A5DC-AAF02D4DDC57}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{C83A05C2-F5AF-4a7b-87B3-6EBDE07B3B43}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{EDF78E1B-3142-4c6e-AD40-0AF0D0D55C63}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
\CLSID\{F5AB293C-2E31-4441-9AD6-B346EE26DF5}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{0D14687F-FA35-465D-B716-BCBC1F9A92D3}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{12813770-461E-4A9F-6C5B-C227A8E9F5B8}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{1180C24E-F5BF-4BB4-AF4C-BBB610B62638}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{A1647E8-5EC2-49FE-B632-E12D765FA00C}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{2DECFC09-D910-4BAC-94B8-FC066827A60F}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{4AA76F27-81BC-4C3F-9F24-CB90749C8CC9}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{59399E43-FB51-48AB-8AE4-AE108B36DAB4}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{6813BFFD-BE81-4611-B4E6-FA1ED0DA8659}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{CA36000-3320-49D1-BAD1-4C5169D4084A}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{15A1949-500C-45F3-A106-34FE03F491EF}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{2DAE9202-0019-4D30-A4D2-AAF02D1DDC37}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{A0ECCE5AB-C02F-489B-BD7B-53C229F774F3}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{A91616B1-1EB0-4051-B519-0A40C2204380}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface
\{CFC09FCE-C963-49E5-A3A4-0A31FFFE1E55}
```

Adds the value:

to the registry subkey:

so that the risk runs every time Windows starts.

to the registry subkey:

**Attachment C**

©1995 - 2008 Symantec Corporation

[Site Map](#)

[Legal Notices](#)

[Privacy Policy](#)

[Contact Us](#)

[Global Sites](#)

[License  
Agreements](#)



## Spyware Information: WinAntiSpyware

This application is **adware**. Adware is not normally a threat, but is usually considered a nuisance. It might have been installed by another application. It can pop up advertisements even if you have a popup blocker on your computer. It can monitor your computer usage to generate ads that you are more likely to respond to. Adware can consume processing power and network bandwidth, thus slowing down your computer and interrupting your workflow.

- Size: 7,793,920 bytes
- Threat level: Medium (more info...)
- Detections: 8,833 this month: 78
- Author: WinSoftware
- Others by this author: WinFixer, WinAntiVirus
- Appeared: 09/05/2005

## Research

- Method of infection: WinAntiSpyware has been installed by other malicious applications and via drive by active-X.
- Advertising: WinAntiSpyware uses false positives to trick the user into believing their computer is infected with a virus. WinAntiSpyware is sometimes installed with real viruses to scare the user into purchasing the full version in order to remove the virus.
- Stability issues: WinAntiSpyware runs as a background process and installs files into the system directory. Because it runs as a background process and nests itself into the operating system it may cause stability problems.

## Spyware Detection Stats

- Spyware Fingerprints: 91,859
- Detections: 6,758,527
- Detections this Month: 4,528

## Spyware Search

Enter Spyware Name

## Recommended

Keep your computer safe. Automatically keeps up-to-date to protect from the latest threats.





## Spyware matching "winantispysware"

- WinAntiSpyware
  - Category: Adware
  - Detections: 8,833

## Suspicious files matching "winantispysware"

- winantispysware2006freeinstall[1].exe
  - Detections: 160
  - Comments: 0
- winantispysware2007freeinstall[1].exe
  - Detections: 33
  - Comments: 0
- winantispysware2007freeinstall.exe
  - Detections: 13
  - Comments: 0
- winantispysware2006setup.exe
  - Detections: 12
  - Comments: 0
- winantispyswarescannerinstall[1].exe
  - Detections: 6
  - Comments: 0
- winantispysware2006freeinstall\_fr[1].exe
  - Detections: 5
  - Comments: 0
- winantispyswarescannerinstall.exe
  - Detections: 3
  - Comments: 0
- winantispysware2006freeinstall2[1].exe
  - Detections: 2
  - Comments: 0
- winantispysware2006freeinstall[2].exe
  - Detections: 2
  - Comments: 0
- winantispysware2007setup.exe
  - Detections: 2
  - Comments: 0
- winantispysware 2007 freeinstall.exe
  - Detections: 2
  - Comments: 0

- Spyware Fingerprints: 91,859
- Detections: 6,758,527
- Detections this Month: 4,528

## Spyware Search

winantispysware

Submit

## Recommended



**SpyCatcher™**

Keep your computer safe. Automatically keeps up-to-date to protect from the latest threats.



## Spyware Information: AdvancedCleaner

This application is **adware**. Adware is not normally a threat, but is usually considered a nuisance. It might have been installed by another application. It can pop up advertisements even if you have a popup blocker on your computer. It can monitor your computer usage to generate ads that you are more likely to respond to. Adware can consume processing power and network bandwidth, thus slowing down your computer and interrupting your workflow.

- Size: Unknown
- Threat level: Low (more info...)
- Detections: 265 this month: 1

## Research

- Method of infection: AdvancedCleaner may be installed through exploits in the Windows Operating system or downloaded manually from the product's website.
- Advertising: Displays exaggerated reports to scare users into purchasing the full version of their software.

## Spyware Detection Stats

- Spyware Fingerprints: 91,859
- Detections: 6,758,527
- Detections this Month: 4,528

## Spyware Search

Enter Spyware Name

Search

## Recommended

Keep your computer safe. Automatically keeps up-to-date to protect from the latest threats.





## Spyware Information: WinAntiVirus

This application is **adware**. Adware is not normally a threat, but is usually considered a nuisance. It might have been installed by another application. It can pop up advertisements even if you have a popup blocker on your computer. It can monitor your computer usage to generate ads that you are more likely to respond to. Adware can consume processing power and network bandwidth, thus slowing down your computer and interrupting your workflow.

- Size: 1,043,311 bytes
- Threat level: Medium (more info...)
- Detections: 6,991 this month: 21
- Author: WinSoftware
- Others by this author: WinFixer
- Appeared: 09/05/2005

## Research

- Method of infection: WinAntiVirus has been installed by other malicious applications and via drive by active-X.
- Advertising: WinAntiVirus uses false positives to trick the user into believing their computer is infected with a virus. WinAntiVirus is sometimes installed with real viruses to scare the user into purchasing the full version in order to remove the virus.
- Stability issues: WinAntiVirus runs as a background process and installs files into the system directory. Because it runs as a background process and nests itself into the operating system it may cause stability problems.

## Spyware Detection Stats

- Spyware Fingerprints: 91,859
- Detections: 6,758,527
- Detections this Month: 4,528

## Spyware Search

Enter Spyware Name

## Recommended

Keep your computer safe. Automatically keeps up-to-date to protect from the latest threats.





## Spyware matching "winantivirus"

- ✱ WinAntiVirus
  - ✱ Category: Adware
  - ✱ Detections: 6,991
- ✱ WinAntiVirus 2005
  - ✱ Category: Adware
  - ✱ Detections: 165
- ✱ WinAntiVirus Pro 2007
  - ✱ Category: Adware
  - ✱ Detections: 1,924

## Suspicious files matching "winantivirus"

- ✱ winantiviruspro2006freeinstall[1].exe
  - ✱ Detections: 514
  - ✱ Comments: 0
- ✱ winantiviruspro2007freeinstall[1].exe
  - ✱ Detections: 61
  - ✱ Comments: 0
- ✱ winantiviruspro2006freeinstall\_de[1].exe
  - ✱ Detections: 41
  - ✱ Comments: 1
- ✱ winantiviruspro2006scannerinstall[1].exe
  - ✱ Detections: 36
  - ✱ Comments: 0
- ✱ ~winantivirus2005setup.exe
  - ✱ Detections: 28
  - ✱ Comments: 0
- ✱ winantiviruspro2006freeinstall\_se[1].exe
  - ✱ Detections: 13
  - ✱ Comments: 0
- ✱ winantiviruspro2007freeinstall.exe
  - ✱ Detections: 13
  - ✱ Comments: 0
- ✱ winantiviruspro2006freeinstall\_no[1].exe
  - ✱ Detections: 11
  - ✱ Comments: 0
- ✱ winantiviruspro2006freeinstall\_it[1].exe
  - ✱ Detections: 10
  - ✱ Comments: 0
- ✱ winantivirus2005proinstall[1].exe
  - ✱ Detections: 8

- Comments: 0
- winantiviruspro2006freeinstall.exe
  - Detections: 7
  - Comments: 0
- winantiviruspro2006freeinstall[2].exe
  - Detections: 5
  - Comments: 0
- winantiviruspro2006freeinstall\_br[1].exe
  - Detections: 5
  - Comments: 0
- winantiviruspro2006freeinstall\_fr[1].exe
  - Detections: 4
  - Comments: 0
- winantiviruspro2006setup[1].exe
  - Detections: 4
  - Comments: 0
- winantivirus.pro[1].exe
  - Detections: 3
  - Comments: 0
- winantiviruspro2006freeinstall\_dk[1].exe
  - Detections: 3
  - Comments: 0
- winantiviruspro2006freeinstall\_jp[1].exe
  - Detections: 3
  - Comments: 0
- ~winantivirussetup.exe
  - Detections: 2
  - Comments: 0
- winantiviruspro2006installer[1].exe
  - Detections: 2
  - Comments: 0
- winantiviruspro2006setup\_de[1].exe
  - Detections: 2
  - Comments: 0
- winantiviruspro2006installer.exe
  - Detections: 2
  - Comments: 0
- winantiviruspro2006freeinstall\_nl[1].exe
  - Detections: 2
  - Comments: 0
- winantiviruspro2006freeinstall\_es[1].exe
  - Detections: 2
  - Comments: 0
- winantiviruspro2006freeinstall\_sd[1].exe
  - Detections: 2
  - Comments: 0
- winantiviruspro2006freeinstall[6].exe

Detections: 2

Comments: 0

## Spyware Detection Stats

Spyware Fingerprints: 91,859

Detections: 6,758,527

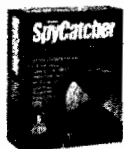
Detections this Month: 4,528

## Spyware Search

winantivirus

Submit

## Recommended



**SpyCatcher™**

Keep your computer safe. Automatically keeps up-to-date to protect from the latest threats.



## Spyware Information: DriveCleaner

This application is **adware**. Adware is not normally a threat, but is usually considered a nuisance. It might have been installed by another application. It can pop up advertisements even if you have a popup blocker on your computer. It can monitor your computer usage to generate ads that you are more likely to respond to. Adware can consume processing power and network bandwidth, thus slowing down your computer and interrupting your workflow.

- Size: 1,939,664 bytes
- Threat level: Low (more info...)
- Detections: 2,805 this month: 4

## Research

- Method of infection: DriveCleaner can be installed through ActiveX controls in popup ads or downloaded from the product website.
- Advertising: DriveCleaner flags numerous benign system entries as dangerous files and goads the user into purchasing the full version by exaggerating the risk present on the system.

## Spyware Detection Stats

- Spyware Fingerprints: 91,859
- Detections: 6,758,527
- Detections this Month: 4,528

## Spyware Search

Enter Spyware Name

Search

## Recommended

Keep your computer safe. Automatically keeps up-to-date to protect from the latest threats.





## Spyware matching "drivecleaner"

- ▶ DriveCleaner
  - ▶ Category: Adware
  - ▶ Detections: 2,805

## Suspicious files matching "drivecleaner"

- ✱ installdrivecleanerstart[1].exe
  - ▶ Detections: 414
  - ▶ Comments: 0
- ✱ setupdrivecleanerstart[1].exe
  - ▶ Detections: 10
  - ▶ Comments: 0
- ✱ installdrivecleanerstart\_no[1].exe
  - ▶ Detections: 10
  - ▶ Comments: 0
- ✱ installdrivecleanerstart[2].exe
  - ▶ Detections: 6
  - ▶ Comments: 0
- ✱ installdrivecleanerstart.exe
  - ▶ Detections: 4
  - ▶ Comments: 0
- ✱ installdrivecleanerstart\_fr[1].exe
  - ▶ Detections: 4
  - ▶ Comments: 0
- ✱ installdrivecleanerstart\_de[1].exe
  - ▶ Detections: 3
  - ▶ Comments: 0
- ✱ installdrivecleanerstart\_es[1].exe
  - ▶ Detections: 2
  - ▶ Comments: 0
- ✱ installdrivecleanerstart[10].exe
  - ▶ Detections: 2
  - ▶ Comments: 0
- ✱ installdrivecleanerstart[11].exe
  - ▶ Detections: 2
  - ▶ Comments: 0
- ✱ installdrivecleanerstart[12].exe
  - ▶ Detections: 2
  - ▶ Comments: 0
- ✱ installdrivecleanerstart[13].exe
  - ▶ Detections: 2

- ↳ Comments: 0
- installdrivecleanerstart[14].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[15].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[16].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[17].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[18].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[19].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[20].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[3].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[4].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[5].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[6].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[7].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[8].exe
  - ↳ Detections: 2
  - ↳ Comments: 0
- installdrivecleanerstart[9].exe
  - ↳ Detections: 2
  - ↳ Comments: 0

## Spyware Detection Stats

• Spyware Fingerprints: 91,859

Page 214

Attachment C

Detections: 6,758,527

Detections this Month: 4,528

## Spyware Search

drivecleaner

Submit

## Recommended



**SpyCatcher™**

Keep your computer safe. Automatically keeps up-to-date to protect from the latest threats.

The United States was firmly in the lead in potentially unwanted software detections in 2H07 with 63.9 million detections in 2H07, nearly six times as many as any other country. The United Kingdom, Canada, and Australia rank third, seventh, and thirteenth, respectively, reflecting the predominance of English-language potentially unwanted software programs. China had the second highest number of detections with 11.1 million detections, up from 4.6 million detections in 1H07, due in part to increased adoption of Chinese-language versions of the detection tools.

#### *Rogue Security Software*

Rogue security software exploits computer users' anxieties about malicious software with fraudulent offers of "protection" for a price. Rogue security software uses a number of different techniques to attempt to trick users into installing the software and to obtain money from them. The prevalence of rogue security software continues to increase, with many common families being delivered by trojan downloaders and other malware, as well as by conventional social engineering methods.

FIGURE 49. Top 25 rogue security software families in 2H07, by number of detections

| Rank | Rogue                     | Volume    |
|------|---------------------------|-----------|
| 1    | Win32/Winfixer            | 3,382,135 |
| 2    | Win32/SpywareSecure       | 610,616   |
| 3    | Win32/SpySheriff          | 569,147   |
| 4    | Win32/WinSoftware         | 384,630   |
| 5    | Win32/VirusProtectpro     | 219,685   |
| 6    | Win32/UltimateDefender    | 210,970   |
| 7    | Win32/Contravirus         | 157,798   |
| 8    | Win32/DriveCleaner        | 153,857   |
| 9    | Win32/AdvancedCleaner     | 134,533   |
| 10   | Win32/AntivirusGold       | 121,954   |
| 11   | Win32/AntiVirGear         | 120,352   |
| 12   | Win32/UltimateCleaner     | 118,559   |
| 13   | Win32/VirusRanger         | 97,221    |
| 14   | Win32/SpyAxe              | 91,864    |
| 15   | Win32/SpyLocked           | 80,898    |
| 16   | Win32/SpyHeal             | 59,534    |
| 17   | Win32/SystemDoctor        | 44,181    |
| 18   | Win32/VirusLocker         | 41,081    |
| 19   | Win32/SpyCrush            | 35,697    |
| 20   | Win32/AntivirusProtection | 33,156    |
| 21   | Win32/AntispyStorm        | 32,513    |
| 22   | Win32/UltimateFixer       | 26,408    |
| 23   | Win32/EZCatch             | 26,219    |
| 24   | Win32/SpywareStormer      | 20,849    |
| 25   | Win32/ErrorGuard          | 19,314    |

# McAfee SiteAdvisor

**McAfee SECURE Shopping****Shop Now >**Want to add your comments? [Log in](#) or [Register](#)[HOME](#)[DOWNLOAD](#)[ANALYSIS](#)[SUPPORT](#)[BLOG](#)[ABOUT US](#)Look up a site report: 

## advancedcleaner.com



In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

Are you the owner of this site? [Leave a comment](#)

Contact information:

Popularity

  
A few users

**Watch all 3 FOR FREE!**  
with enrollment in a Free Triple Advantage™ Trial Membership

Monitor all 3 of your national credit reports.  
Plus get a Free Experian® Credit Report & Score.

**One Month!**

### AUTOMATED WEB SAFETY TESTING RESULTS FOR ADVANCEDCLEANER.COM

E-MAIL TESTS FOR ADVANCEDCLEANER.COM: ?

DOWNLOAD TESTS FOR ADVANCEDCLEANER.COM: ?

#### 4 red downloads

In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

[View detailed analysis](#)[Submit a download for analysis](#)[See how McAfee can protect your PC from dangerous downloads.](#)

#### Downloads we found on this site:

##### Download

ADCFreeInstaller.exe  
ADCFreeInstaller.exe  
ADCFreeInstaller.exe  
ADCFreeInstaller.ni.exe  
ADCFreeInstaller.exe

10 total downloads. [See more.](#)

##### Analysis

Generic Downloader.x trojan  
Generic Downloader.x trojan  
Downloader.gen trojan  
Generic Downloader.x trojan  
AdvancedCleaner

ONLINE AFFILIATIONS FOR ADVANCEDCLEANER.COM: ?

#### Linked to green site

When we visited this site, we found that most of its links are to sites which are safe or have only minor safety/annoyance issues.

[adult-billing.com](#)[advancedcleaner.com](#)

ANNOYANCES FROM ADVANCEDCLEANER.COM: ?

1 popup

Page 217

REVIEWER AND WEB SITE OWNER COMMENTS

ATTACHMENT E

## USER REVIEW SUMMARY FOR ADVANCEDCLEANER.COM ?

**Risky downloads [Reported]**

Feedback from credible users suggests that downloads on this site may contain what some people would consider adware, spyware, or other potentially unwanted programs.

|                                  |                             |
|----------------------------------|-----------------------------|
| This site is slow (0)            | Excessive redirects (0)     |
| This site spams (1)              | Phishing or other scams (1) |
| Adware, spyware, or viruses (18) | Bad shopping experience (0) |
| Browser exploit (1)              |                             |



## ADVANCEDCLEANER.COM WEB SITE OWNER COMMENTS (0) ?

Are you the owner of this site? Add a comment

## USER REVIEWS (21) ?

page 1 of 3

Learn more about our reviewer system.

Rating: Adware, spyware, or viruses

Malware domain!

Typ: Rogue Software download

This domain is used to spear "Rogue Software".

##### What is "Rogue Software"? #####

Rogue Software are computer applications which tries to trick you by telling you, that you are infected with spyware and/or viruses. But in truth you are just infected with this "Rogue Software". The malicious application tells you that the installed "Antivirus" or "Antispyware" application is just a demo version and that you have to buy the full version of the software to remove the virus / spyware from you computer. The truth is, that you are not infected. They just want to make money with your fear! Such malicious applications are also known as:

- Rogue Antivirus
- Rogue Software
- Rogue security software
- Rogue security application
- Fake security application

Normally the Rogue applicaiton changes your wallpaper and installs a fake bluescreen as screensaver (desktop hijacking).

Such "fake security applications" are promoted with many different names:

- AdwarePatrol
- AdwareRemover
- AntivirusXP 2008
- AntivirusXP 2009
- Antivirus 2009 Professional
- XP Security Center
- XP Antivirus 2009
- IE Defender
- WinFixer
- WinSpywareProtect
- Spyware Warrior
- Spyware Remover
- etc....

It's all the same crap! For more information take a look at  
[http://en.wikipedia.org/wiki/Rogue\\_software](http://en.wikipedia.org/wiki/Rogue_software)

##### Why is this software "Rogue"? #####

1. First of all the software don't ask you if you would like to install the applications - it just do it!
2. The malware says that you are infected with malware. Yeah, maybe thats true but the application DOESN'T remove the detected viruses from your machine!
3. The application fakes alert messages and bluescreens
4. They try to trap you by offering a "free spwayware/malware/virus" scan

5. There is a "Uninstall" button where you "can" uninstall the software. Well, when you press the button the software just removes the uninstall button! The application still stays on your computer and shows you faked alert messages and bluescreens!

#### ##### How to get infected #####

There are two different ways you can get infected with such malicious applications:

Normally you get "infected" thru a malicious download (like in this case). But there are also well known malware which reloads such Rogue software after the infection (like wsnpoem / zbot do this). That's really suspicious!

#### ##### How to remove Rogue Software #####

Just download and install Malwarebytes "RogueRemover" from  
<http://www.malwarebytes.org/rogueremover.php> (The application is for free).

#### ##### How to fight against malware #####

Submit Malware to MIRT: <http://www.castlecops.com/mirt>  
Download & install Spybot S&D: <http://www.safer-networking.org/en/download/>  
Download & Run McAfee Rootkit Detective: <http://vil.nai.com/VIL/STINGER/RKSTINGER.ASPX>  
Download & install Lavasoft Ad-Aware: [http://lavasoft.com/products/ad\\_aware\\_free.php](http://lavasoft.com/products/ad_aware_free.php)

Posted at 10/01/2008-12:35:10 AM by SaMsX, Experienced Reviewer View profile [ Reputation score: 9 / 9 ]

Rating: Adware, spyware, or viruses

#### Listed @ Malware Domainlist:

<http://www.malwaredomainlist.com/mdl.php?search=advancedcleaner.com&colsearch=All&quantity=50>

Current IP\*: 84.243.252.147

IP PTR: box2.bugaganetwork.com

::Name Servers::

ns1.advancedcleaner.com

ns2.advancedcleaner.com

ns3.advancedcleaner.com

ns4.advancedcleaner.com

::Dates & Status::

Created Date 2007-01-16 12:33:08 EST

Updated Date 2008-01-16 20:07:31 EST

Valid Date 2009-01-16 12:33:08 EST

Posted at 08/13/2008-02:01:44 AM by TeMerc, Experienced Reviewer View profile [ Reputation score: 9 / 9 ]

Rating: Adware, spyware, or viruses

Posted at 07/26/2008-10:21:56 PM by adr14nf, Reviewer View profile [ Reputation score: 1 / 9 ]

Rating: Adware, spyware, or viruses

#### This site is also rated as 'Malicious' by Trusted Source:

<http://www.trustedsource.org/TS?do=feedback&subdo=query&q=advancedcleaner.com>

Users should use caution when viewing this site

Posted at 07/06/2008-03:39:23 AM by TeMerc, Experienced Reviewer View profile [ Reputation score: 9 / 9 ]

Rating: Adware, spyware, or viruses

Posted at 04/01/2008-09:30:31 PM by tetak, Reviewer View profile [ Reputation score: 9 / 9 ]

Rating: Adware, spyware, or viruses

Address seems to currently redirect to another red-rated site?

<http://www.siteadvisor.com/sites/turvapc.com>

Either that or they identify my geographic area, and try to infest me with malware that speaks my language ...

Posted at 03/23/2008-06:37:16 AM by lordpake, Experienced Reviewer | View profile | Reputation score: 0 / 0

Rating: Adware, spyware, or viruses

**my grandfather had it**

Posted at 03/22/2008-05:21:13 PM by korri123, Reviewer | View profile | Reputation score: 0 / 0

Rating: Adware, spyware, or viruses

**<http://it.advancedcleaner.com/cleaner/installer.php>**

Posted at 02/17/2008-03:55:44 AM by DBill, Reviewer | View profile | Reputation score: 0 / 0

Rating: Adware, spyware, or viruses

**Rogue Software, contain viruses and Adware , Steer clear from this site!**

Posted at 02/11/2008-06:26:22 PM by iTaLyPwNs, Reviewer | View profile | Reputation score: 1 / 0

Rating: This site spams

**In addition to virus and spyware, this site also spams. The slime-ball spammer has posted numerous posts on a G-rated forum I'm active on. Anyone opening the post, gets an eyefull of hard-core porn.**

**\*\*\*\*\*ANYONE WHO VISITS THIS SITE IS AT RISK OF BEING INFECTED, EVEN IF YOU DONT DOWNLOAD ANYTHING\*\*\*\*\***

Posted at 02/11/2008-11:47:04 AM by brian218, Reviewer | View profile | Reputation score: 1 / 0

page 1 of 3

User Name

☐ Remember Me?

Password

Not a reviewer, yet? [Register](#) and leave a review of this site.

Get fully protected with **McAfee Internet Security Suite**.

Copyright © 2008 McAfee, Inc.

[Home](#) [Download](#) [Analysis](#) [Support](#) [About us](#) [Privacy policy](#) [Terms of service](#) [Site Owner info](#) [Blog](#)

[Pick a language](#)

# McAfee SiteAdvisor



McAfee SECURE Shopping

Shop Now >

Want to add your comments? Log in or Register.

HOME DOWNLOAD ANALYSIS SUPPORT BLOG ABOUT US

Look up a site report

## drivecleaner.com



In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

Are you the owner of this site? Leave a comment

Contact information:

Country Popularity



Canada



Many users

Experience the Power of 3  
**FOR FREE!**  
with enrollment in Triple Advantage<sup>SM</sup>  
3-Bureau Credit Monitoring.  
Plus get a  
Free Experian<sup>®</sup> Credit Report & Score!

### AUTOMATED WEB SAFETY TESTING RESULTS FOR DRIVECLEANER.COM

E-MAIL TESTS FOR DRIVECLEANER.COM: ?

DOWNLOAD TESTS FOR DRIVECLEANER.COM: ?

#### 24 red downloads

In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

[View detailed analysis](#)

[Submit a download for analysis](#)

[See how McAfee can protect your PC from dangerous downloads.](#)

#### Downloads we found on this site:

##### Download

(install)drivecleanerstart.exe  
DriveCleaner 2006 1.0.44.0 (setup)drivecle  
DriveCleaner 2006 Free 1.0.44.3 (install)dr  
DriveCleaner 2006 Free 1.0.44.3 (install)dr  
DriveCleaner 2006 Free 1.0.44.4 (install)dr

25 total downloads. [See more.](#)

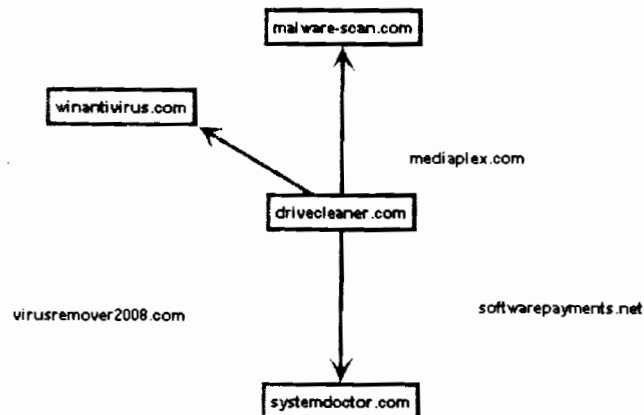
##### Analysis

Winfixer trojan,Downloader.gen trojan  
Winfixer  
DriveCleaner,Winfixer  
DriveCleaner,Winfixer  
DriveCleaner,Winfixer

ONLINE AFFILIATIONS FOR DRIVECLEANER.COM: ?

#### Linked to green sites

When we visited this site, we found that most of its links are to sites which are safe or have only minor safety annoyance issues.



ANNOYANCES FROM DRIVECLEANER.COM: ?

REVIEWER AND WEB SITE OWNER COMMENTS

USER REVIEW SUMMARY FOR DRIVECLEANER.COM: ?

Page 221

ATTACHMENT E

**Negative behaviors. [Reported]**

Feedback from credible users indicates this site engaged in one or more negative or undesired activities.

|                                  |                              |
|----------------------------------|------------------------------|
| This site is good (2)            | Excessive popups (13)        |
| This site spams (1)              | Phishing or other scams (19) |
| Adware, spyware, or viruses (65) | Bad shopping experience (2)  |
| Browser exploit (20)             |                              |

**DRIVECLEANER.COM WEB SITE OWNER COMMENTS (1) ?**

None

Submitted by a1a23 at 2007-07-25 14:20:00

**USER REVIEWS (135) ?**

page 1 of 14

Learn more about our reviewer system.

Rating: Adware, spyware, or viruses

**Evil Bad Poison Death... clean drives? more like burn them**

Posted at 10/20/2008-10:06:03 PM by billy1273, Reviewer . View profile [ Reputation score: 0 - 9 ]

Rating: Phishing or other scams

**DriveCleaner tries to convince you that you need a scan, but it's not true! And based on the sites it links to, it appears to be a WinFixer site.**

Posted at 08/20/2008-06:06:18 PM by virusflagger, Reviewer . View profile [ Reputation score: 1 - 9 ]

**WinFixer Inc. Maker of thos websites:**

Drivecleaner.com  
 Anti-virus-pro.com  
 Anti-spyware-pro.com  
 Anti-rootkits-pro.com  
 And more...

**All that programs are the same rogue!****Info Found By: Bunneling**

Posted at 07/14/2008-10:00:38 AM by Bunneling, Reviewer . View profile [ Reputation score: 1 - 9 ]

Rating: Browser exploit

**Drive Cleaner took over my browser and i couldn't go on to any page....but i used Avast....AND IT BLOCKED THAT TOO!!!! I NEED HELP PLEASE!!**

Posted at 05/25/2008-03:54:27 PM by StormKiller, Reviewer . View profile [ Reputation score: 1 - 9 ]

Rating: Adware, spyware, or viruses

**rogue**

Posted at 04/13/2008-06:31:25 PM by Xanderzone365, Reviewer . View profile [ Reputation score: 0 - 9 ]

Rating: Adware, spyware, or viruses

**I hate this site. It keeps popping up on websites. Twice it has done a drive-by download on my computer.**

Posted at 04/10/2008-01:04:44 PM by Sheepz, Reviewer . View profile [ Reputation score: 0 - 9 ]

Rating: Adware, spyware, or viruses

Don't download any files from this website!

Help protect your PC from malware found on this site by installing Windows Defender (Windows XP only) from

<http://www.microsoft.com/athome/security/spyware/software/default.msp>

Posted at 02/23/2008-09:38:35 PM by tetak, Reviewer, View profile, Reputation score: 9 / 9

Rating: Flashing or other scams

its because of site like this that try to install spyware onto your computer, that we use mcafee.

Posted at 02/10/2008-06:28:53 AM by yellow13, Reviewer, View profile, Reputation score: 1 / 9

Rating: Adware, spyware, or viruses

busy with wrong and illegal things.

Posted at 01/01/2008-12:09:38 PM by nathansf, Reviewer, View profile, Reputation score: 1 / 9

This website is bad. It is promoting fake SCAM software that's pretending to be real security software.

Don't buy any of their worthless stuff. If your computer is sending you to this SCAM SITE using alert balloons, pop-ups, a browser toolbar, or a hijack of your browser or your desktop screen, then you need to clean your computer with REAL antivirus and REAL antispyware software.

~ REMOVAL OF INFECTION ~

One easy way to remove an infection is System Restore. In Windows XP or Windows Vista, click Start > All Programs > Accessories > System Tools > System Restore, and "go back in time" to before you got infected. Also follow the steps below, then see the security tips at the end so this doesn't keep happening.

SUPERAntiSpyware spyware-removal software:  
<http://www.superantispyware.com>

Spybot Search & Destroy spyware-removal software:  
<http://www.safer-networking.org>

SmitFraudFix is an advanced tool that targets this sort of stuff, follow the directions carefully if you use it:  
[http://siri.urz.free.fr/Fix/SmitfraudFix\\_En.php](http://siri.urz.free.fr/Fix/SmitfraudFix_En.php)

Panda AntiRootkit, rootkit remover:  
[http://www.majorgeeks.com/Panda\\_Anti-Rootkit\\_d5457.html](http://www.majorgeeks.com/Panda_Anti-Rootkit_d5457.html)

Update your virus definitions, then run a full antivirus scan. Besides your own antivirus software, also get a "second opinion" from some additional online antivirus scanners, such as these:

<http://support.f-secure.com/enu/home/ols.shtml>  
<http://www.pandasoftware.com/products/activescan.htm>  
<http://housecall.trendmicro.com>

You can uproot stubborn stuff manually using HijackThis, if the antivirus and antispyware scanners don't detect it. Start Windows in Safe Mode to use HijackThis (HJT) most effectively. If you get an error when you run HJT, rename it to something random and run it again (some malware will block it by name):

<http://www.spywareinfo.com/~merijn/programs.php> (download HJT from here)  
<http://hijackthis.de/en> (online HJT logfile analyzer)

To start Windows in Safe Mode so you can run HijackThis properly, begin tapping the F8 key when you know the first Windows startup screen is about to show, the one with the scrolling bar.

## ~ SECURITY TIPS ~

Update your Windows and Office software with security patches:  
<http://update.microsoft.com>

Use Secunia's new checkup tool to see if your computer needs updates for third-party software like QuickTime, Adobe Reader, WinAmp, IM, torrent clients, etc (the bad guys target these nowadays):  
<https://psi.secunia.com>

How to start using defense-in-depth at home:  
<http://home.comcast.net/~mechbgon>

>:(

Posted at 01/01/2008-12:04:43 PM by nathansf. Reviewer [View profile | Reputation score: 1 / 5]

Page 1 of 14

User Name  Remember Me? ☐

Password

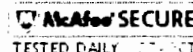
Not a reviewer, yet? Register and leave a review of this site.

Get fully protected with McAfee Internet Security Suite.

Copyright © 2008 McAfee, Inc.

[Home](#) [Download](#) [Analysis](#) [Support](#) [About us](#) [Privacy policy](#) [Terms of service](#) [Site Owner Info](#) [Blog](#)

[Pick a language](#)

[Privacy policy](#)[Terms of Service](#)[Site Owner Info](#)[Contact us](#)[McAfee Home](#)**McAfee SiteAdvisor****McAfee SECURE Shopping****Shop Now >**[Want to add your comments? Log in or Register](#)[Look up a site report:](#) [HOME](#)[DOWNLOAD](#)[ANALYSIS](#)[SUPPORT](#)[BLOG](#)[ABOUT US](#)**errorprotector.com**

In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

Are you the owner of this site? [Leave a comment](#)

Contact information:

Country Popularity



Canada



A few users

**McAfee SECURE Shopping**

Your Secure Shopping Destination  
with Hundreds of Merchants

**Shop Now >**

ALL SITES ARE

**AUTOMATED WEB SAFETY TESTING RESULTS FOR ERRORPROTECTOR.COM****E-MAIL TESTS FOR ERRORPROTECTOR.COM: ?****DOWNLOAD TESTS FOR ERRORPROTECTOR.COM: ?****3 red downloads**

In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

[View detailed analysis](#)[Submit a download for analysis](#)[See how McAfee can protect your PC from dangerous downloads.](#)**Downloads we found on this site:****Download**

ErrorProtector 1.1.145.4 (Install-Errorprote

ErrorProtector 1.1.145.4 (Install-Errorprote

ErrorProtector 1.1.145.5 (Install-Errorprote

**Analysis**

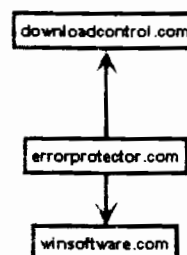
Winfixer trojan

Winfixer trojan

Winfixer trojan, Generic trojan

**ONLINE AFFILIATIONS FOR ERRORPROTECTOR.COM: ?****Linked to red sites**

When we tested this site we found links to winsoftware.com, which we found to be a distributor of downloads some people consider adware, spyware or other potentially unwanted programs.

**ANNOYANCES FROM ERRORPROTECTOR.COM: ?****REVIEWER AND WEB SITE OWNER COMMENTS**

## USER REVIEW SUMMARY FOR ERRORPROTECTOR.COM ?

**Risky downloads [Reported]**

Feedback from credible users suggests that downloads on this site may contain what some people would consider adware, spyware, or other potentially unwanted programs.

This site is good (0)

Excessive ads (0)

This site harms (0)

Phishing or other scams (0)

Adware, spyware, or viruses (8)

Bad shopping experience (0)

Browser exploit (0)



## ERRORPROTECTOR.COM WEB SITE OWNER COMMENTS (0) ?

Are you the owner of this site? Add a comment

## USER REVIEWS (11) ?

page 1 of 2

Learn more about our reviewer system.

Rating: Adware, spyware, or viruses

**What the other reviewers said.**

Posted at 09/26/2008-04:34:42 PM by famcafee, Experienced Reviewer . View profile | Reputation score: 9 / 9 |

Rating: Adware, spyware, or viruses

**Malware domain!**

Typ: Rogue Software download

This domain is used to spear "Rogue Software".

##### What is "Rogue Software"? #####

Rogue Software are computer applications which tries to trick you by telling you, that you are infected with spyware and/or viruses. But in truth you are just infected with this "Rogue Software". The malicious application tells you that the installed "Antivirus" or "Antispyware" application is just a demo version and that you have to buy the full version of the software to remove the virus / spyware from you computer. The truth is, that you are not infected. They just want to make money with your fear! Such malicious applications are also known as:

- Rogue Antivirus
- Rogue Software
- Rogue security software
- Rogue security application
- Fake security application

Normally the Rogue applicaiton changes your wallpaper and installs a fake bluescreen as screensaver (desktop hijacking).

Such "fake security applications" are promoted with many different names:

- AdwarePatrol
- AdwareRemover
- AntivirusXP 2008
- AntivirusXP 2009
- Antivirus 2009 Professional
- XP Security Center
- XP Antivirus 2009
- IE Defender
- WinFixer
- WinSpywareProtect
- Spyware Warrior
- Spyware Remover
- etc....

It's all the same crap! For more information take a look at [http://en.wikipedia.org/wiki/Rogue\\_software](http://en.wikipedia.org/wiki/Rogue_software)

##### Why is this software "Rogue"? #####

1. First of all the software don't ask you if you would like to install the applications - it just do it!
2. The malware says that you are infected with malware. Yeah, maybe thats true but the application DOESN'T remove the detected viruses from your machine!
3. The application fakes alert messages and bluescreens
4. They try to trap you by offering a "free spwayware/malware/virus" scan
5. There is a "Uninstall" button where you "can" uninstall the software. Well, when you press the button the software just removes the uninstall button! The application still stays on you computer and shows you faked alert messages and bluescreens!

#### ##### How to get infected #####

There are two different ways you can get infected with such malicious applications:

Normally you get "infected" thru a malicious download (like in this case). But there are also well known malware which reloads such Rogue software after the infection (like wsnpoem / zbot do this). That's really suspicious!

#### ##### How to remove Rogue Software #####

Just download and install Malwarebytes "RogueRemover" from  
<http://www.malwarebytes.org/rogueremover.php> (The application is for free).

#### ##### How to fight against malware #####

Submit Malware to MIRT: <http://www.castlecops.com/mirt>  
 Download & install Spybot S&D: <http://www.safer-networking.org/en/download/>  
 Download & Run McAfee Rootkit Detective: <http://vil.nai.com/VIL/STINGER/RKSTINGER.ASPX>  
 Download & install Lavasoft Ad-Aware: [http://lavasoft.com/products/ad\\_aware\\_free.php](http://lavasoft.com/products/ad_aware_free.php)

Posted at 09/25/2008-09:51:25 AM by SaMsX, Experienced Reviewer | View profile | Reputation score: 9 / 9 |

Rating: Adware, spyware, or viruses

**Avoid this site at all costs!**

**Downloads Trojans to you PC.**

Posted at 07/04/2008-11:05:43 AM by eXaByTe, Reviewer | View profile | Reputation score: 2 / 9 |

Rating: Adware, spyware, or viruses

**WinFixer**

Posted at 10/31/2007-02:33:35 PM by ANoobishAV, Reviewer | View profile | Reputation score: 1 / 9 |

Rating: Phishing or other scams

mechBgon is all correct. Well, in my suggestion, this fake software may look like that infamous ErrorSafe, because the prefix looks synonymous to that bogus company. Maybe, it's the same suspects that created ErrorSafe before.

Posted at 09/07/2007-06:26:24 AM by threat devas18tr, Reviewer | View profile | Reputation score: 2 / 9 |

Rating: Phishing or other scams

**This website is bad. It is promoting fake SCAM software that's pretending to be real security software.**

**Don't buy any of their worthless stuff. If your computer is sending you to this SCAM SITE using alert balloons, pop-ups, a browser toolbar, or a hijack of your browser or your desktop screen, then you need to clean your computer with REAL antivirus and REAL antispyware software.**

#### **~ REMOVAL OF INFECTION ~**

One easy way to remove an infection is System Restore. In Windows XP or Windows Vista, click Start > All Programs > Accessories > System Tools > System Restore, and "go back in time" to before you got infected. Also follow the steps below, then see the security tips at the end so this doesn't keep happening.

SUPERAntiSpyware spyware-removal software:

**ATTACHMENT E**

**Page 227**

<http://www.superantispyware.com>

**Spybot Search & Destroy** spyware-removal software:

<http://www.safer-networking.org>

**SmitFraudFix** is an advanced tool that targets this sort of stuff, follow the directions carefully if you use it:

<http://siri.urz.free.fr/Fix/SmitfraudFix...En.php>

**Panda AntiRootkit**, rootkit remover:

[http://www.majorgeeks.com/Panda\\_Anti-Rootkit\\_d5457.html](http://www.majorgeeks.com/Panda_Anti-Rootkit_d5457.html)

Update your virus definitions, then run a full antivirus scan. Besides your own antivirus software, also get a "second opinion" from some additional online antivirus scanners, such as these:

<http://support.f-secure.com/enu/home/ois.shtml>

<http://www.pandasoftware.com/products/activescan.htm>

<http://housecall.trendmicro.com>

If antivirus and anti-spyware programs can't completely kill the infection, then you can uproot stubborn stuff manually using HijackThis. Start Windows in Safe Mode to use HijackThis (HJT) most effectively. If you get an error when you run HJT, rename it to something random and run it again (some malware will block it by name):

<http://www.spywareinfo.com/~merijn/programs.php> (download HJT from here)

<http://hijackthis.de/en> (online HJT logfile analyzer, shows you which things to kill)

To start Windows in Safe Mode so you can run HijackThis properly, begin tapping the F8 key when you know the first Windows startup screen is about to show, the one with the scrolling bar. You may need to use Safe Mode With Networking so you can use the online logfile analyzer to show you what to kill.

#### ~ SECURITY TIPS ~

Update your Windows and Office software with security patches:

<http://update.microsoft.com>

Use Secunia's new checkup tool to see if your computer needs updates for third-party software like QuickTime, Adobe Reader, WinAmp, IM, torrent clients, etc (the bad guys target these nowadays):

<https://psi.secunia.com>

How to start using defense-in-depth at home:

<http://home.comcast.net/~mechbgon>

Posted at 09/02/2007-06:37:27 PM by mechBggon, Experienced Reviewer . View profile [ Reputation score: 9 / 9 ]

Rating: Advise, spyware, or viruses

**Dont download put a trojan horse on labtop**

Posted at 07/24/2007-10:12:27 PM by racerapj, Reviewer . View profile [ Reputation score: 1 / 9 ]

Rating: Advise, spyware, or viruses

**Another rogue site. Application is simmilar to that of drivecleaner. Avoid by all cost**

Posted at 06/01/2007-12:16:37 PM by sparsha, Reviewer . View profile [ Reputation score: 9 / 9 ]

Rating: Advise, spyware, or viruses

**A very bad site, avoid at all costs.**

Posted at 05/27/2007-09:47:08 PM by Fleep11, Reviewer . View profile [ Reputation score: 1 / 9 ]

A follow-up that I should have included in my review. Sunbelt Software classifies ErrorProtector as a rogue security program. For more information, see:

<http://research.sunbelt-software.com:threatdisplay.aspx?threatid=44657>

Posted at 04/06/2007-03:50:49 PM by dean, Experienced Reviewer View profile Reputation score 4.9

page 1 of 2

User Name

☐ Remember Me?

Password

Not a reviewer, yet? [Register and leave a review of this site.](#)

Get fully protected with **McAfee Internet Security Suite**.

© Copyright 2008 McAfee, Inc.

[Home](#) [Download](#) [Analysis](#) [Support](#) [About us](#) [Privacy policy](#) [Terms of service](#) [Site Owner info](#) [Blog](#)

[Pick a language](#)

## McAfee SiteAdvisor



McAfee SECURE Shopping

Shop Now &gt;

HOME

DOWNLOAD

ANALYSIS

SUPPORT

BLOG

ABOUT US

Want to add your comments? Log in or Register

Look up a site report

## winadblocker.com



In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

Are you the owner of this site? Leave a comment

Contact information:

Country Popularity



Canada



A few users

**Watch all 3 FOR FREE!**  
with enrollment in a free Triple Advantage™ Trial Membership

Monitor all 3 of your national credit reports.  
Plus get a Free Experian® Credit Report & Score.

**ONE MONTH**

## AUTOMATED WEB SAFETY TESTING RESULTS FOR WINADBLOCKER.COM

E-MAIL TESTS FOR WINADBLOCKER.COM: ?

DOWNLOAD TESTS FOR WINADBLOCKER.COM: ?

## 3 red downloads

In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

View detailed analysis

Submit a download for analysis

See how McAfee can protect your PC from dangerous downloads.

## Downloads we found on this site:

| Download                                | Analysis |
|-----------------------------------------|----------|
| WinAdBlocker 2005 Trial 2.0.25.1 (WinAd | WinFixer |
| WinAdBlocker 2005 Trial 2.0.25.1 (WinAd | WinFixer |
| WinAdBlocker 2005 Trial 2.0.25.1 (WinAd | WinFixer |

ONLINE AFFILIATIONS FOR WINADBLOCKER.COM: ?

ANNOYANCES FROM WINADBLOCKER.COM: ?

## REVIEWER AND WEB SITE OWNER COMMENTS

USER REVIEW SUMMARY FOR WINADBLOCKER.COM: ?

Excellent (0)

Excellent owner (0)

Fair (0)

Phishing or other scams (0)

Adware, spyware, or viruses (2)

Bad shopping experience (0)

Browser exploit (0)

**McAfee SECURE Shopping**  
Shop Now >

Your Secure Shopping  
Destination with  
Hundreds of Merchants

ALL SITES ARE  
McAfee SECURE

WINADBLOCKER.COM WEB SITE OWNER COMMENTS (0) ?

Are you the owner of this site? Add a comment

USER REVIEWS (2) ?

Learn more about our reviewer system.

Rating: Adware, spyware, or viruses

Malware domain!

page 1 of 1

ATTACHMENT E

Page 230

Typ: Rogue Software download

This domain is used to spear "Rogue Software".

##### What is "Rogue Software"? #####

Rogue Software are computer applications which tries to trick you by telling you, that you are infected with spyware and/or viruses. But in truth you are just infected with this "Rogue Software". The malicious application tells you that the installed "Antivirus" or "Antispyware" application is just a demo version and that you have to buy the full version of the software to remove the virus / spyware from you computer. The truth is, that you are not infected. They just want to make money with your fear! Such malicious applications are also known as:

- Rogue Antivirus
- Rogue Software
- Rogue security software
- Rogue security application
- Fake security application

Normally the Rogue applicaiton changes your wallpaper and installs a fake bluescreen as screensaver (desktop hijacking).

Such "fake security applications" are promoted with many different names:

- AdwarePatrol
- AdwareRemover
- AntivirusXP 2008
- AntivirusXP 2009
- Antivirus 2009 Professional
- XPSecurity Center
- XPAntivirus 2009
- IEDefender
- WinFixer
- WinSpywareProtect
- Spyware Warrior
- Spyware Remover
- etc....

It's all the same crap! For more information take a look at

[http://en.wikipedia.org/wiki/Rogue\\_software](http://en.wikipedia.org/wiki/Rogue_software)

##### Why is this software "Rogue"? #####

1. First of all the software don't ask you if you would like to install the applications - it just do it!
2. The malware says that you are infected with malware. Yeah, maybe thats true but the application DOESNT remove the detected viruses from your machine!
3. The application fakes alert messages and bluescreens
4. They try to trap you by offering a "free spwayware/malware/virus" scan
5. There is a "Uninstall" button where you "can" uninstall the software. Well, when you press the button the software just removes the uninstall button! The application still stays on you computer and shows you faked alert messages and bluescreens!

##### How to get infected #####

There are two different ways you can get infected which such malicious applications:

Normally you get "infected" thru a malicious download (like in this case). But there are also well known malware which reloads such Rogue software after the infection (like wsnpoem / zbot do this). That's really suspicious!

##### How to remove Rogue Software #####

Just download and install Malwarebytes "RogueRemover" from

<http://www.malwarebytes.org/rogueremover.php> (The application is for free).

##### How to fight against malware #####

Submit Malware to MIRT: <http://www.castlecops.com/mirt>

Download & install Spybot S&D: <http://www.safer-networking.org/en/download/>

Download & Run McAfee Rootkit Detective: <http://vil.nai.com/VIL/STINGER/RKSTINGER.ASPX>

Download & install Lavasoft Ad-Aware: [http://lavasoft.com/products/ad\\_aware\\_free.php](http://lavasoft.com/products/ad_aware_free.php)

Posted at 09/25/2008-09:48:06 AM by SaMsX, Experienced Reviewer View profile Reputation score: 9 / 9

### Principles of Learning and Memory

Be careful when visiting this site. It's part of the Winsoftware family and installing it will cost your pc.

Posted at 09/11/2007-11-48 06 PM by threat devast8tr. Reviewer View profile : Reputation score: 2 / 91

Page 1 of 1

User Name   User Name

## Remember Me?

Password

Log in

**Not a reviewer, yet? Register and leave a review of this site.**

Get fully protected with McAfee Internet Security Suite.

Copyright © 2008 M. A. Greer et al.

[Home](#)   [Download](#)   [Analysis](#)   [Support](#)   [About us](#)   [Privacy policy](#)   [Terms of service](#)   [Site Owner Info](#)   [Blog](#)

Pick a language

McAfee SiteAdvisor



McAfee SECURE Shopping

Shop Now &gt;

[HOME](#) [DOWNLOAD](#) [ANALYSIS](#) [SUPPORT](#) [BLOG](#) [ABOUT US](#)
Want to add your comments? [Log in](#) or [Register](#)

Look up a site report

## winantispyspy.com



When we tested this site we found links to winantispyspyware.com, which we found to be a distributor of downloads some people consider adware, spyware or other potentially unwanted programs.

Are you the owner of this site? [Leave a comment](#)

Contact information:

Country Popularity



Canada



A few users

**Experience the Power of 3  
FOR FREE!**  
 with enrollment in Triple Advantage<sup>SM</sup>  
 3-Bureau Credit Monitoring.  
**Plus get a**  
 Free Experian<sup>®</sup> Credit Report & Score!

## AUTOMATED WEB SAFETY TESTING RESULTS FOR WINANTISPY.COM

E-MAIL TESTS FOR WINANTISPY.COM: ?

DOWNLOAD TESTS FOR WINANTISPY.COM: ?

ONLINE AFFILIATIONS FOR WINANTISPY.COM: ?

## Linked to red site

When we tested this site we found links to winantispyspyware.com, which we found to be a distributor of downloads some people consider adware, spyware or other potentially unwanted programs.



ANNOYANCES FROM WINANTISPY.COM: ?

## REVIEWER AND WEB SITE OWNER COMMENTS

USER REVIEW SUMMARY FOR WINANTISPY.COM ?

## Negative behaviors. [Reported]

Feedback from some users indicated this site engaged in one or more negative or undesired activities

This site is slow (0)

Excessive popups (0)

This site uploads (0)

Phishing or other scams (0)

Adware, spyware, or viruses (1)

Bad shopping experience (1)

Browser extensions (0)

ATTACHMENT E

Page 233



WINANTISPY.COM WEB SITE OWNER COMMENTS (0) ?

Are you the owner of this site? Add a comment

USER REVIEWS (2) ?

Page 1 of 1

Learn more about our reviewer system.

Rating: Adware, spyware, or viruses

**Malware domain!**

**Typ: Rogue Software download**

This domain is used to spear "Rogue Software".

##### What is "Rogue Software"? #####

Rogue Software are computer applications which tries to trick you by telling you, that you are infected with spyware and/or viruses. But in truth you are just infected with this "Rogue Software". The malicious application tells you that the installed "Antivirus" or "Antispyware" application is just a demo version and that you have to buy the full version of the software to remove the virus / spyware from you computer. The truth is, that you are not infected. They just want to make money with your fear! Such malicious applications are also known as:

- Rogue Antivirus
- Rogue Software
- Rogue security software
- Rogue security application
- Fake security application

Normaly the Rogue applicaiton changes your wallpaper and installs a fake bluescreen as screensaver (desktop hijacking).

Such "fake security applications" are promoted with many different names:

- AdwarePatrol
- AdwareRemover
- AntivirusXP 2008
- AntivirusXP 2009
- Antivirus 2009 Professional
- XP Security Center
- XP Antivirus 2009
- IE Defender
- WinFixer
- WinSpywareProtect
- Spyware Warrior
- Spyware Remover
- etc....

It's all the same crap! For more information take a look at

[http://en.wikipedia.org/wiki/Rogue\\_software](http://en.wikipedia.org/wiki/Rogue_software)

##### Why is this software "Rogue"? #####

1. First of all the software don't ask you if you would like to install the applications - it just do it!
2. The malware says that you are infected with malware. Yeah, maybe thats true but the application DOESN'T remove the detected viruses from your machine!
3. The application fakes alert messages and bluescreens
4. They try to trap you by offering a "free spwayware/malware/virus" scan
5. There is a "Uninstall" button where you "can" uninstall the software. Well, when you press the button the software just removes the uninstall button! The application still stays on you computer and shows you faked alert messages and bluescreens!

##### How to get infected #####

There are two different ways you can get infected which such malicious applications:

ATTACHMENT E

Page 234

Normaly you get "infected" thru a malicious download (like in this case). But there are also well known malware which reloads such Rogue software after the infection (like wsnpoem / zbot do this). That's really suspicious!

##### How to remove Rogue Software #####

Just download and install Malwarebytes "RogueRemover" from  
<http://www.malwarebytes.org/rogueremover.php> (The application is for free).

##### How to fight against malware #####

Submit Malware to MIRT: <http://www.castlecops.com/mirt>  
Download & install Spybot S&D: <http://www.safer-networking.org/en/download/>  
Download & Run McAfee Rootkit Detective: <http://vil.nai.com/VIL/STINGER/RKSTINGER.ASPX>  
Download & install Lavasoft Ad-Aware: [http://lavasoft.com/products/ad\\_aware\\_free.php](http://lavasoft.com/products/ad_aware_free.php)

Posted at 09/25/2008-09:48:42 AM by SaMsX, Experienced Reviewer | View profile | Reputation score: 9 / 9 |

Rating: Bad shopping experience

Distributes rogue antispyware apps. The same program is also distributed through these sites

[softwareprofit.com](http://softwareprofit.com)  
[winantispayware.com](http://winantispayware.com)  
[winantivirus.com](http://winantivirus.com)  
[winfixer.com](http://winfixer.com)  
[winsoftware.com](http://winsoftware.com)

See:

[http://www.spywarewarrior.com/rogue\\_anti-spyware.htm](http://www.spywarewarrior.com/rogue_anti-spyware.htm)

Posted at 04/18/2006-09:51:58 AM by dean, Experienced Reviewer | View profile | Reputation score: 9 / 9 |

page 1 of 1

User Name

☐ Remember Me?

Password

Not a reviewer, yet? [Register and leave a review of this site.](#)

Get fully protected with **McAfee Internet Security Suite**.

McAfee SiteAdvisor



McAfee SECURE Shopping

Shop Now &gt;

HOME

DOWNLOAD

ANALYSIS

SUPPORT

BLOG

ABOUT US

Want to add your comments? Log in or Register.

Look up a site report:

winantispware.com



In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

Are you the owner of this site? Leave a comment

Contact information:

Country

Popularity



Canada



A few users

McAfee SECURE Shopping

Your Secure Shopping Destination  
with Hundreds of Merchants

Shop Now &gt;

ALL SITES ARE



## AUTOMATED WEB SAFETY TESTING RESULTS FOR WINANTISPYWARE.COM

## E-MAIL TESTS FOR WINANTISPYWARE.COM: ?

## DOWNLOAD TESTS FOR WINANTISPYWARE.COM: ?!

## 10 red downloads

In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

[View detailed analysis](#)

[Submit a download for analysis](#)

[See how McAfee can protect your PC from dangerous downloads.](#)

## Downloads we found on this site:

## Download

(WinAntiSpyware2007FreeInstall.exe)

WinAntiSpyware 2005 3.0.17.0 (WinAntiS

WinAntiSpyware 2005 3.0.26.4 (WinAntiS

WinAntiSpyware 2006 (Unregistered versi

WinAntiSpyware 2006 3.0.28.4 (Demo) (V

## Analysis

Generic trojan

WinFixer

WinFixer,Generic PUP.i

Winfixer,BackDoor-BAC trojan

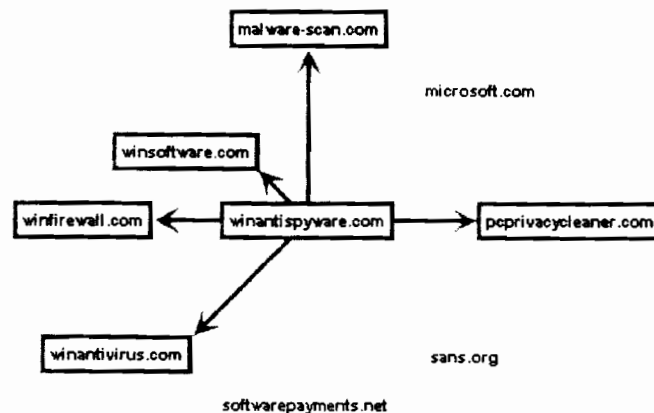
WinFixer

12 total downloads. See more.

## ONLINE AFFILIATIONS FOR WINANTISPYWARE.COM: ?!

## Linked to red sites

When we tested this site we found links to winsoftware.com, which we found to be a distributor of downloads some people consider adware, spyware or other potentially unwanted programs.



## ANNOYANCES FROM WINANTISPYWARE.COM: ?

## REVIEWER AND WEB SITE OWNER COMMENTS

ATTACHMENT E

Page 236

## USER REVIEW SUMMARY FOR WINANTISPYWARE.COM ?

**Negative behaviors. [Reported]**

Feedback from some users indicated this site engaged in one or more negative or undesired activities.

|                                  |                             |
|----------------------------------|-----------------------------|
| This site is good (0)            | Excessive popups (0)        |
| This site spams (2)              | Phishing or other scams (4) |
| Adware, spyware, or viruses (24) | Bad shopping experience (2) |
| Browser exploit (3)              |                             |



## WINANTISPYWARE.COM WEB SITE OWNER COMMENTS (0) ?

Are you the owner of this site? Add a comment

## USER REVIEWS (35) ?

page 1 of 4

Learn more about our reviewer system.

Rating: Adware, spyware, or viruses

Posted at 10/11/2008-10:47:44 AM by Matty0364, Reviewer View profile [ Reputation score: 0 / 9 ]

Rating: Phishing or other scams

This site offers false antivirus software (rougeware). It also can redirect to <http://www.oczyszczaczkomputerza.com> (another malicious site). Both offer to download WinFixer malware variants.

Posted at 10/05/2008-03:57:53 PM by InfoProf, Reviewer View profile [ Reputation score: 1 / 9 ]

Rating: Adware, spyware, or viruses

**Malware domain!**

**Typ: Rogue Software download**

This domain is used to spear "Rogue Software".

##### What is "Rogue Software"? #####

Rogue Software are computer applications which tries to trick you by telling you, that you are infected with spyware and/or viruses. But in truth you are just infected with this "Rogue Software". The malicious application tells you that the installed "Antivirus" or "Antispyware" application is just a demo version and that you have to buy the full version of the software to remove the virus / spyware from you computer. The truth is, that you are not infected. They just want to make money with your fear! Such malicious applications are also known as:

- Rogue Antivirus
- Rogue Software
- Rogue security software
- Rogue security application
- Fake security application

Normally the Rogue applicaiton changes your wallpaper and installs a fake bluescreen as screensaver (desktop hijacking). Such "fake security applications" are promoted with many different names:

- AdwarePatrol
- AdwareRemover
- AntivirusXP 2008
- AntivirusXP 2009
- Antivirus 2009 Professional
- XP Security Center
- XP Antivirus 2009
- IE Defender
- WinFixer
- WinSpywareProtect
- Spyware Warrior

-Spyware Remover  
etc....

It's all the same crap! For more information take a look at  
[http://en.wikipedia.org/wiki/Rogue\\_software](http://en.wikipedia.org/wiki/Rogue_software)

##### Why is this software "Rogue"? #####

1. First of all the software don't ask you if you would like to install the applications - it just do it!
2. The malware says that you are infected with malware. Yeah, maybe thats true but the application DOESN'T remove the detected viruses from your machine!
3. The application fakes alert messages and bluescreens
4. They try to trap you by offering a "free spwayware/malware/virus" scan
5. There is a "Uninstall" button where you "can" uninstall the software. Well, when you press the button the software just removes the uninstall button! The application still stays on you computer and shows you faked alert messages and bluescreens!

##### How to get infected #####

There are two different ways you can get infected which such malicious applications:

Normaly you get "infected" thru a malicious download (like in this case). But there are also well known malware which reloads such Rogue software after the infection (like wsnpoem / zbot do this). That's realy suspicious!

##### How to remove Rogue Software #####

Just download and install Malwarebytes "RogueRemover" from  
<http://www.malwarebytes.org/rogueremover.php> (The application is for free).

##### How to fight against malware #####

Submit Malware to MIRT: <http://www.castlecops.com/mirt>  
Download & install Spybot S&D: <http://www.safer-networking.org/en/download/>  
Download & Run McAfee Rootkit Detective: <http://vil.nai.com/VIL/STINGER/RKSTINGER.ASPX>  
Download & install Lavasoft Ad-Aware: [http://lavasoft.com/products/ad\\_aware\\_free.php](http://lavasoft.com/products/ad_aware_free.php)

Posted at 09/25/2008-09:53:46 AM by SaMsX, Experienced Reviewer . View profile [ Reputation score: 9 / 9 ]

Rating: Adware, spyware, or viruses

This site uses scare tactics to scare an inexperienced user to download it by saying: YOUR COMPUTER IS INFECTED!!!!!! YOUR ANTI-VIRUS DOES NOT WORK!!!!!!WE FOUND 257 INFECTED OBJECTS!!!!!! You might get to this website because of a pop-up that "LOOKS" like a valid windows security warning box. This is the first step....of your computers dimised. It'll ask you if you want to download and install it with 2 buttons that say: yes or no. DO NOT FALL FOR THE TRAP!!!! BOTH OF THE BOTTONS ARE YES!!! IF YOU CLICK NO IT'LL FORCE YOU TO INSTALL IT ANYWAY!....To prevent this....when you receive the pop-up...don't click on anything!!!! Pull out your internet connection from your computer...then close the pop-up by clicking the X botton on the corner! YOU HAVE BEEN WARNED!!!!

Posted at 02/17/2008-06:03:30 PM by Computer GEEEEEEEEEEK, Reviewer . View profile [ Reputation score: 1 / 9 ]

Rating: Adware, spyware, or viruses

**Avoid this site at all costs!**

Posted at 12/28/2007-09:28:41 AM by Sporzafanaat, Reviewer . View profile [ Reputation score: 1 / 9 ]

Rating: Adware, spyware, or viruses

this site is the same as winfixer.com  
i advise to block winfixer sites with a firewall software

Posted at 10/16/2007-07:31:34 PM by ANoobishAV, Reviewer . View profile [ Reputation score: 1 / 9 ]

Rating: Adware, spyware, or viruses

Posted at 10/13/2007-02:37:16 PM by P.L, Reviewer . View profile [ Reputation score: 1 / 9 ]

Rating: Adware, spyware, or viruses

**Warning:** This site contains dangerous software like Spyware, Adware, Backdoors and Downloading Agents.

**NEVER, EVER VISIT THIS BAD SITE EN ESPECIALLY DO NOT DOWNLOAD SOMETHING. IF YOU VISITED IT, DELETE YOUR TEMPORARY FILES AND COOKIES AND MAKE SOME BACKUPS OF YOUR IMPORTANT FILES, JUST TO BE SURE.**

Posted at 09/29/2007-09:04:50 AM by DenDuDe, Reviewer | View profile | Reputation score: 1 - 9 |

Rating: Adware, spyware, or viruses

i told it no i didnt want a virus scan and it opened a new browser anyways. ihis pos probaly did a drive by download so i mite haqv 2 redo my comp AGAIN!

Posted at 09/24/2007-05:01:53 PM by rampagingidiot2, Reviewer | View profile | Reputation score: 1 - 9 |

Rating: Adware, spyware, or viruses

**I never even went to their website and it automatically downloaded onto my work computer. My work computer crashed the next day.**

Posted at 09/15/2007-10:50:55 PM by fencerdavid2007, Reviewer | View profile | Reputation score: 1 - 9 |

page 1 of 4

User Name

☐ Remember Me?

Password

Not a reviewer, yet? [Register and leave a review of this site.](#)

Get fully protected with **McAfee Internet Security Suite**.

Copyright ©2008 McAfee, Inc.

[Home](#) | [Download](#) | [Analysis](#) | [Support](#) | [About us](#) | [Privacy policy](#) | [Terms of service](#) | [Site Owner Info](#) | [Blog](#)

[Pick a language](#)

McAfee SiteAdvisor™



McAfee SECURE Shopping

Shop Now &gt;

Want to add your comments? Log in or Register

Look up a site report

HOME

DOWNLOAD

ANALYSIS

SUPPORT

BLOG

ABOUT US

## winantivirus.com



In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

Are you the owner of this site? Leave a comment

Contact information:

Country Popularity



Canada



Some users

McAfee SECURE Shopping

Your Secure Shopping Destination  
with Hundreds of Merchants

Shop Now &gt;

ALL SITES ARE



## AUTOMATED WEB SAFETY TESTING RESULTS FOR WINANTIVIRUS.COM

## E-MAIL TESTS FOR WINANTIVIRUS.COM: ?

## DOWNLOAD TESTS FOR WINANTIVIRUS.COM: ?

## 30 red downloads

In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

[View detailed analysis](#)

[Submit a download for analysis](#)

[See how McAfee can protect your PC from dangerous downloads.](#)

## Downloads we found on this site:

## Download

WinAntiVirus 2005 Pro 1.1.91.2 (WinAntiVirus)  
WinAntiVirus Pro 2006 2.0.220.0 (WinAntiVirus)  
WinAntiVirus Pro 2006 2.1.271.0 (WA6Pir)  
WinAntiVirus Pro 2006 2.1.271.0 (WinAntiVirus)  
WinAntiVirus Pro 2006 (WinAntiVirusPro2)

38 total downloads. See more.

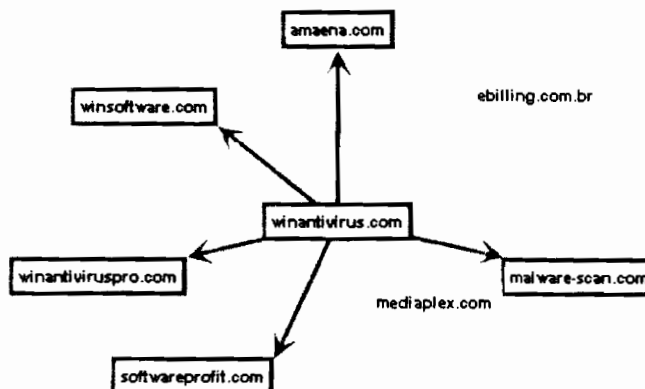
## Analysis

WinFixer  
Generic trojan, WinFixer  
Winfixer  
Winfixer, Generic Delphi trojan  
Generic trojan, Winfixer

## ONLINE AFFILIATIONS FOR WINANTIVIRUS.COM: ?

## Linked to red sites

When we tested this site we found links to winsoftware.com, which we found to be a distributor of downloads some people consider adware, spyware or other potentially unwanted programs



## ANNOYANCES FROM WINANTIVIRUS.COM: ?



1 popup

## REVIEWER AND WEB SITE OWNER COMMENTS

## USER REVIEW SUMMARY FOR WINANTIVIRUS.COM ?

**Misleading site. [Reported]**

Feedback from some users indicated this site engaged in one or more negative or undesired activities.

|                                  |                              |
|----------------------------------|------------------------------|
| This site is good (3)            | Excessive popups (3)         |
| This site spams (3)              | Phishing or other scams (22) |
| Adware, spyware, or viruses (89) | Bad shopping experience (4)  |
| Browser exploit (8)              |                              |



## WINANTIVIRUS.COM WEB SITE OWNER COMMENTS (0) ?

Are you the owner of this site? Add a comment

## USER REVIEWS (145) ?

page 1 of 15

Learn more about our reviewer system.

Rating: Adware, spyware, or viruses

**Adware! just look at allyboo148's review it explains all**

Posted at 10/20/2008-10:00:18 PM by billy1273, Reviewer . View profile [ Reputation score: 0 - 9 ]

Rating: Adware, spyware, or viruses

**Dj, just shut up. Win Antivirus PRETENDS to be Windows Anti-Virus, but it isn't.**

Posted at 10/19/2008-12:34:10 PM by Zangosucks2, Reviewer . View profile [ Reputation score: 1 - 9 ]

Rating: Adware, spyware, or viruses

**Rogue domain.**

Posted at 10/04/2008-07:17:18 AM by Zangosucks2, Reviewer . View profile [ Reputation score: 1 - 9 ]

Rating: Adware, spyware, or viruses

**Malware domain!**

Typ: Rogue Software download

This domain is used to spear "Rogue Software".

##### What is "Rogue Software"? #####

Rogue Software are computer applications which tries to trick you by telling you, that you are infected with spyware and/or viruses. But in truth you are just infected with this "Rogue Software". The malicious application tells you that the installed "Antivirus" or "Antispyware" application is just a demo version and that you have to buy the full version of the software to remove the virus / spyware from you computer. The truth is, that you are not infected. They just want to make money with your fear! Such malicious applications are also known as:

- Rogue Antivirus
- Rogue Software
- Rogue security software
- Rogue security application
- Fake security application

Normaly the Rogue applicaiton changes your wallpaper and installs a fake bluescreen as screensaver (desktop hijacking).

Such "fake security applications" are promoted with many different names:

- AdwarePatrol
- AdwareRemover
- AntivirusXP 2008

-AntivirusXP 2009  
 -Antivirus 2009 Professional  
 -XP Security Center  
 -XP Antivirus 2009  
 -IE Defender  
 -WinFixer  
 -WinSpywareProtect  
 -Spyware Warrior  
 -Spyware Remover  
 etc....

It's all the same crap! For more information take a look at  
[http://en.wikipedia.org/wiki/Rogue\\_software](http://en.wikipedia.org/wiki/Rogue_software)

#### ##### Why is this software "Rogue"? #####

1. First of all the software don't ask you if you would like to install the applications - it just do it!
2. The malware says that you are infected with malware. Yeah, maybe thats true but the application DOESN'T remove the detected viruses from your machine!
3. The application fakes alert messages and bluescreens
4. They try to trap you by offering a "free spwayware/malware/virus" scan
5. There is a "Uninstall" button where you "can" uninstall the software. Well, when you press the button the software just removes the uninstall button! The application still stays on you computer and shows you faked alert messages and bluescreens!

#### ##### How to get infected #####

There are two different ways you can get infected with such malicious applications:

Normally you get "infected" thru a malicious download (like in this case). But there are also well known malware which reloads such Rogue software after the infection (like wsnpoem / zbot do this). That's really suspicious!

#### ##### How to remove Rogue Software #####

Just download and install Malwarebytes "RogueRemover" from  
<http://www.malwarebytes.org/rogueremover.php> (The application is for free).

#### ##### How to fight against malware #####

Submit Malware to MIRT: <http://www.castlecops.com/mirt>  
 Download & install Spybot S&D: <http://www.safer-networking.org/en/download/>  
 Download & Run McAfee Rootkit Detective: <http://vil.nai.com/VIL/STINGER/RKSTINGER.ASPX>  
 Download & install Lavasoft Ad-Aware: [http://lavasoft.com/products/ad\\_aware\\_free.php](http://lavasoft.com/products/ad_aware_free.php)

Posted at 09/25/2008-09:52:49 AM by SaMsX, Experienced Reviewer . View profile [ Reputation score: 9 / 9 ]

Rating: Adware, spyware, or viruses

Posted at 09/09/2008-11:55:39 PM by BeCautiousPeople, Reviewer . View profile [ Reputation score: 2 / 9 ]

Rating: This site is good

its exactly what it says:

If you wanted winDOWS antivirus you should have typed that instead.

Posted at 07/27/2008-07:16:59 AM by Djdin, Reviewer . View profile [ Reputation score: 0 / 9 ]

Rating: Adware, spyware, or viruses

winfixer is a rogue software like macsweeper.

Posted at 07/04/2008-03:48:11 AM by Popop100, Reviewer . View profile [ Reputation score: 0 / 9 ]

Rating: Adware, spyware, or viruses

Winfixer is BACK!

Posted at 07/01/2008-09:15:00 PM by Reprotected, Reviewer . View profile [ Reputation score: 7 / 9 ]

Rating: Adware, spyware, or viruses

**Adware. An enthusiast. An exorcist. A criminal.**

If you want to help prevent adware, warn people about the dangers. Spread the word. If you find a virus, report it to a agency. If you know a criminal, report him. Save Our Computers.

If you want to know more about malware, there are sites out there that can teach you.

<http://sunbeltblog.blogspot.com/>

<http://lockergnome.com/>

<http://kasperskylabs.com/>

We can all put effort into this. If we can stop it, we will know how to stop all malware.

Help us!

Posted at 06/15/2008-07:57:22 PM by Protectzor, Reviewer . View profile { Reputation score: 1 / 9 }

Rating: Adware, spyware, or viruses

**Rogue app**

Posted at 06/11/2008-10:18:08 PM by kage akuma, Reviewer . View profile { Reputation score: 0 / 9 }

page 1 of 15

User Name

☐ Remember Me?

Password

Not a reviewer, yet? [Register](#) and leave a review of this site.

Get fully protected with **McAfee Internet Security Suite**.

Copyright © 2008 McAfee, Inc.

[Home](#) [Download](#) [Analysis](#) [Support](#) [About us](#) [Privacy policy](#) [Terms of service](#) [Site Owner Info](#) [Blog](#)

[Pick a language](#)

# McAfee SiteAdvisor



## McAfee SECURE Shopping

[Shop Now >](#)

 Want to add your comments? [Log in](#) or [Register](#)
[HOME](#)[DOWNLOAD](#)[ANALYSIS](#)[SUPPORT](#)[BLOG](#)[ABOUT US](#)
 Lock up a site report: 

### wincontentfilter.com



In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

Are you the owner of this site? [Leave a comment](#)

Contact information:

Country Popularity



Canada



A few users

## McAfee SECURE Shopping

### Your Secure Shopping Destination with Hundreds of Merchants

[Shop Now >](#)

ALL SITES ARE



#### AUTOMATED WEB SAFETY TESTING RESULTS FOR WINCONTENTFILTER.COM

##### E-MAIL TESTS FOR WINCONTENTFILTER.COM: ?

##### DOWNLOAD TESTS FOR WINCONTENTFILTER.COM: ?

###### 3 red downloads

In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

[View detailed analysis](#)
[Submit a download for analysis](#)
[See how McAfee can protect your PC from dangerous downloads.](#)

###### Downloads we found on this site:

###### Download

WinContentFilter 2005 Trial 2.0.37.0 (Win)  
 WinContentFilter 2005 Trial 2.0.37.0 (Win)  
 WinContentFilter 2005 Trial 2.0.37.0 (Win)

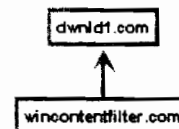
###### Analysis

WinFixer  
 WinFixer  
 WinFixer

##### ONLINE AFFILIATIONS FOR WINCONTENTFILTER.COM: ?

###### Linked to red site

When we tested this site we found links to [dwld1.com](#), which we found to be a distributor or downloads some people consider adware, spyware or other potentially unwanted programs.



##### ANNOYANCES FROM WINCONTENTFILTER.COM: ?

##### REVIEWER AND WEB SITE OWNER COMMENTS

## USER REVIEW SUMMARY FOR WINCONTENTFILTER.COM ?

**Risky downloads [Reported]**

Feedback from credible users suggests that downloads on this site may contain what some people would consider malware, spyware, or other potentially unwanted programs.

|                                 |                             |
|---------------------------------|-----------------------------|
| This site is good (0)           | Excessive popups (0)        |
| This site is bad (0)            | Phishing or other scams (0) |
| Adware, spyware, or viruses (3) | Bad shopping experience (0) |
| Browser exploit (0)             |                             |



## WINCONTENTFILTER.COM WEB SITE OWNER COMMENTS (0) ?

Are you the owner of this site? Add a comment

## USER REVIEWS (3) ?

page 1 of 1

Learn more about our reviewer system.

Rating: Adware, spyware, or viruses

**Malware domain!**

**Typ: Rogue Software download**

**This domain is used to spear "Rogue Software".**

**##### What is "Rogue Software"? #####**

Rogue Software are computer applications which tries to trick you by telling you, that you are infected with spyware and/or viruses. But in truth you are just infected with this "Rogue Software". The malicious application tells you that the installed "Antivirus" or "Antispyware" application is just a demo version and that you have to buy the full version of the software to remove the virus / spyware from you computer. The truth is, that you are not infected. They just want to make money with your fear! Such malicious applications are also known as:

- Rogue Antivirus
- Rogue Software
- Rogue security software
- Rogue security application
- Fake security application

Normally the Rogue applicaiton changes your wallpaper and installs a fake bluescreen as screensaver (desktop hijacking).

Such "fake security applications" are promoted with many different names:

- AdwarePatrol
- AdwareRemover
- AntivirusXP 2008
- AntivirusXP 2009
- Antivirus 2009 Professional
- XPSecurity Center
- XPAntivirus 2009
- IEDefender
- WinFixer
- WinSpywareProtect
- Spyware Warrior
- Spyware Remover
- etc....

It's all the same crap! For more information take a look at  
[http://en.wikipedia.org/wiki/Rogue\\_software](http://en.wikipedia.org/wiki/Rogue_software)

**##### Why is this software "Rogue"? #####**

1. First of all the software don't ask you if you would like to install the applications - it just do it!
2. The malware says that you are infected with malware. Yeah, maybe thats true but the application DOESN'T remove the detected viruses from your machine!
3. The application fakes alert messages and bluescreens
4. They try to trap you by offering a "free spwayware/malware/virus" scan

5. There is a "Uninstall" button where you "can" uninstall the software. Well, when you press the button the software just removes the uninstall button! The application still stays on you computer and shows you faked alert messages and bluescreens!

#### ##### How to get infected #####

There are two different ways you can get infected with such malicious applications:

Normally you get "infected" thru a malicious download (like in this case). But there are also well known malware which reloads such Rogue software after the infection (like wsnpoem / zbot do this). That's really suspicious!

#### ##### How to remove Rogue Software #####

Just download and install Malwarebytes "RogueRemover" from  
<http://www.malwarebytes.org/rogueremover.php> (The application is for free).

#### ##### How to fight against malware #####

Submit Malware to MIRT: <http://www.castlecops.com/mirt>  
 Download & install Spybot S&D: <http://www.safer-networking.org/en/download/>  
 Download & Run McAfee Rootkit Detective: <http://vil.nai.com/VIL/STINGER/RKSTINGER.ASPX>  
 Download & install Lavasoft Ad-Aware: [http://lavasoft.com/products/ad\\_aware\\_free.php](http://lavasoft.com/products/ad_aware_free.php)

Posted at 09/25/2008-09:48:59 AM by SaMsX, Experienced Reviewer | View profile [ Reputation score: 9 / 9 ]

Rating: Adware, spyware, or viruses

Is WinContentFilter dangerous? That's difficult to say. It hasn't shown up in any of the well known databases yet, at least that I am aware of. Given WinSoftware's past history of aggressive and deceptive advertising (see spywarewarrior.com), marketing of rogue apps like WinAntiSpyware and WinAntiVirus along with trial downloads not being available, it seems prudent to avoid anything sold by WinSoftware.

The SiteAdvisor analysis implies that there is a trial download of WinContentFilter available. However, I could not find a link for a trial download on the site.

Other WinSoftware products:

WinAdBlocker - [winadblocker.com](http://winadblocker.com)  
 WinAntiSpam - [winantispam.com](http://winantispam.com)  
 WinAntiSpy - [winantispay.com](http://winantispay.com)  
 WinAntiSpyware - [winantispayware.com](http://winantispayware.com)  
 WinAntiVirus - [winantivirus.com](http://winantivirus.com)  
 WinContentFilter - [wincontentfilter.com](http://wincontentfilter.com)  
 WinDriveCleaner - [windrivecleaner.com](http://windrivecleaner.com)  
 WinFirewall - [winfirewall.com](http://winfirewall.com)  
 WinFixer - [winfixer.com](http://winfixer.com)  
 WinNanny - [winnanny.com](http://winnanny.com)  
 WinPopupGuard - [winpopupguard.com](http://winpopupguard.com)

All the above excepting winantispam.com and wincontentfilter.com are currently rated "red" by SiteAdvisor.

Interesting side-note: The names used for the "testimonials" on the web site are Katty Zolner in Kansas and Samuel Dupious in New York. Those sound like real names, eh? They actually sound a lot more like phony names spammers use. After checking several "white page" sites, I couldn't find ANY examples of these surnames in their respective states. If you can't find an unusual surname in New York, it probably doesn't exist.

Posted at 07/20/2006-09:31:25 AM by dean, Experienced Reviewer | View profile [ Reputation score: 9 / 9 ]

Rating: Adware, spyware, or viruses

Belongs to rogue anti-spyware family. Avoid this with all cost.

Posted at 07/10/2006-07:03:55 AM by TheOdds, Reviewer | View profile [ Reputation score: 1 / 9 ]

Password

[Log in](#)

Not a reviewer, yet? [Register](#) and [leave a review](#) of this site.

Get fully protected with **McAfee Internet Security Suite**.

Copyright © 2008 McAfee, Inc.

[Home](#) [Download](#) [Analysis](#) [Support](#) [About us](#) [Privacy policy](#) [Terms of service](#) [Site Owner Info](#) [Blog](#)

[Pick a language](#)

# McAfee SiteAdvisor



## McAfee SECURE Shopping

[Shop Now >](#)
[Want to add your comments? Log in or Register](#)
[Look up a site report:](#)

[HOME](#)[DOWNLOAD](#)[ANALYSIS](#)[SUPPORT](#)[BLOG](#)[ABOUT US](#)

## windrivecleaner.com



In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

Are you the owner of this site? Leave a comment

Contact information:

Country

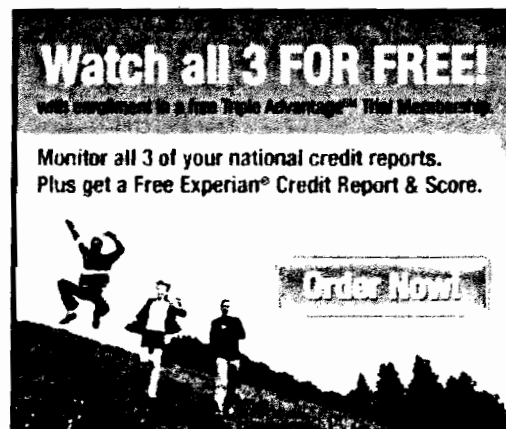
Popularity



Canada



A few users



**Watch all 3 FOR FREE!**  
 with enrollment in a free Triple Advantage™ Trial Membership

Monitor all 3 of your national credit reports.  
 Plus get a Free Experian® Credit Report & Score.

**Order Now!**

### AUTOMATED WEB SAFETY TESTING RESULTS FOR WINDRIVECLEANER.COM

E-MAIL TESTS FOR WINDRIVECLEANER.COM: ?

DOWNLOAD TESTS FOR WINDRIVECLEANER.COM: ?

#### 1 red download

In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

Downloads we found on this site:

Download

WinDriveCleaner 2005 Trial 2.0.55.6 (Win

Analysis

WinFixer

[View detailed analysis](#)

[Submit a download for analysis](#)

[See how McAfee can protect your PC from dangerous downloads.](#)

ONLINE AFFILIATIONS FOR WINDRIVECLEANER.COM: ?

ANNOYANCES FROM WINDRIVECLEANER.COM: ?

### REVIEWER AND WEB SITE OWNER COMMENTS

USER REVIEW SUMMARY FOR WINDRIVECLEANER.COM ?

#### Risky downloads [Reported]

Feedback from credible users suggests that downloads on this site may contain what some people would consider adware, spyware, or other potentially unwanted programs.

This site is good (0)

Excessive popups (0)

This site scams (0)

Phishing or other scams (1)

Adware, spyware, or viruses (2)

Bad shopping experience (0)

Browser exploit (0)



**McAfee SECURE Shopping**

[Shop Now >](#)

Your Secure Shopping Destination with Hundreds of Merchants

ALL SITES ARE  


WINDRIVECLEANER.COM WEB SITE OWNER COMMENTS (0) ?

Are you the owner of this site? Add a comment

USER REVIEWS (5) ?

ATTACHMENT E

Page 248

page 1 of 1

Learn more about our reviewer system.

Rating: A (safe, spyware, or viruses)

Malware domain!

Typ: Rogue Software download

This domain is used to spear "Rogue Software".

##### What is "Rogue Software"? #####

Rogue Software are computer applications which tries to trick you by telling you, that you are infected with spyware and/or viruses. But in truth you are just infected with this "Rogue Software". The malicious application tells you that the installed "Antivirus" or "Antispyware" application is just a demo version and that you have to buy the full version of the software to remove the virus / spyware from you computer. The truth is, that you are not infected. They just want to make money with your fear! Such malicious applications are also known as:

- Rogue Antivirus
- Rogue Software
- Rogue security software
- Rogue security application
- Fake security application

Normally the Rogue applicaiton changes your wallpaper and installs a fake bluescreen as screensaver (desktop hijacking).

Such "fake security applications" are promoted with many different names:

- AdwarePatrol
- AdwareRemover
- AntivirusXP 2008
- AntivirusXP 2009
- Antivirus 2009 Professional
- XPSecurity Center
- XPAntivirus 2009
- IEDefender
- WinFixer
- WinSpywareProtect
- Spyware Warrior
- Spyware Remover
- etc....

It's all the same crap! For more information take a look at  
[http://en.wikipedia.org/wiki/Rogue\\_software](http://en.wikipedia.org/wiki/Rogue_software)

##### Why is this software "Rogue"? #####

1. First of all the software don't ask you if you would like to install the applications - it just do it!
2. The malware says that you are infected with malware. Yeah, maybe thats true but the application DOESN'T remove the detected viruses from your machine!
3. The application fakes alert messages and bluescreens
4. They try to trap you by offering a "free spwayware/malware/virus" scan
5. There is a "Uninstall" button where you "can" uninstall the software. Well, when you press the button the software just removes the uninstall button! The application still stays on you computer and shows you faked alert messages and bluescreens!

##### How to get infected #####

There are two different ways you can get infected which such malicious applications:

Normaly you get "infected" thru a malicious download (like in this case). But there are also well known malware which reloads such Rogue software after the infection (like wsnpoem / zbot do this). That's realy suspicious!

##### How to remove Rogue Software #####

Just download and install Malwarebytes "RogueRemover" from  
<http://www.malwarebytes.org/rogueremover.php> (The application is for free).

##### How to fight against malware #####

Submit Malware to MIRT: <http://www.castlecops.com/mirt>

Download & install Spybot S&D: <http://www.safer-networking.org/en/download/>

Download & Run McAfee Rootkit Detective: <http://vil.nai.com/VIL/STINGER/RKSTINGER.aspx>

Page 249

ATTACHMENT E

Download & install Lavasoft Ad-Aware: [http://lavasoft.com/products/ad\\_aware\\_free.php](http://lavasoft.com/products/ad_aware_free.php)

Posted at 09/25/2008-09:49:18 AM by SaMsX, Experienced Reviewer, View profile [ Reputation score: 10/9 ]

Hey dean. Some of your posts and a post from me had worked=) This site is officially red!

Posted at 09/01/2007-10:13:42 PM by threat devast8tr, Reviewer, View profile [ Reputation score: 2/9 ]

Rating: Adware, spyware or viruses

Almost four months ago I reviewed this site which distributes software from the notorious WinSoftware group, well-known for WinFixer, WinAntivirus, WinAntiSpyware and other rogue apps.

The site is still live. Could someone get a clue please?

Posted at 07/31/2007-08:44:56 AM by dean, Experienced Reviewer, View profile [ Reputation score: 9/9 ]

A follow-up that I should have included in my review. Sunbelt Software classifies WinDriveCleaner as a rogue security program. For more information, see:

<http://research.sunbelt-software.com/threatdisplay.aspx?threatid=44353>

Posted at 04/06/2007-03:51:29 PM by dean, Experienced Reviewer, View profile [ Reputation score: 9/9 ]

Rating: Phishing or other scams

One can only wonder how this site wound up with a green rating. It is run by, or for the benefit of WinSoftware, which has a history of aggressive and deceptive advertising, marketing of rogue apps like WinAntiSpyware and WinAntiVirus and non-availability of trial downloads. SiteAdvisor has already rated at least eighteen other WinSoftware sites RED (see below). It seems prudent to avoid anything sold by them.

Some of their stuff "sells" for as much as \$79.95. Even if any of it was legitimate, the price would be hard to justify. This is a classic rip-off. What follows is a list of other WinSoftware sites. All of these are rated RED by SiteAdvisor.

66.244.254.43 softwareprofit.com  
 66.244.254.46 vantagesoftware.com  
 66.244.254.46 winadblocker.com  
 66.244.254.46 winantispam.com  
 66.244.254.46 winantispy.com  
 66.244.254.46 wincontentfilter.com  
 66.244.254.46 winfirewall.com (green, unfortunately)  
 66.244.254.46 winnanny.com  
 66.244.254.46 winpopupguard.com (green, unfortunately)  
 66.244.254.46 winsoftware.com  
 66.244.254.63 amaena.com  
 66.244.254.63 errorprotector.com (unrated)  
 66.244.254.63 internetantispy.com  
 66.244.254.63 nortoncomparison.com  
 66.244.254.63 virusguard.com  
 66.244.254.63 winantivirus.com  
 66.244.254.63 winpluspak.com  
 66.244.254.64 amaena.com  
 66.244.254.64 internetantispy.com  
 66.244.254.64 personalantispy.com (unrated)  
 66.244.254.64 virusguard.com  
 66.244.254.64 winantispyware.com  
 66.244.254.177 mcafeereview.com  
 66.244.254.177 qualitysoftware.com

Posted at 04/06/2007-07:18:29 AM by dean, Experienced Reviewer, View profile [ Reputation score: 9/9 ]

Page 1 of 1

User Name

☐ Remember Me?

Password

Not a reviewer, yet? [Register and leave a review of this site.](#)

Get fully protected with **McAfee Internet Security Suite**.

Copyright © 2008 McAfee, Inc.

[Home](#)

[Download](#)

[Analysis](#)

[Support](#)

[About us](#)

[Privacy policy](#)

[Terms of service](#)

[See Owner info](#)

[Blog](#)

[Pick a language](#)

**McAfee SiteAdvisor****McAfee SECURE Shopping**[Shop Now >](#)[Want to add your comments? Log in or Register](#)[Look up a site report:](#) [HOME](#)[DOWNLOAD](#)[ANALYSIS](#)[SUPPORT](#)[BLOG](#)[ABOUT US](#)**winfixer.com**

When we tested this site we found links to winsoftware.com, which we found to be a distributor of downloads some people consider adware, spyware or other potentially unwanted programs.

Are you the owner of this site? [Leave a comment](#)

Contact information: Country Popularity



-



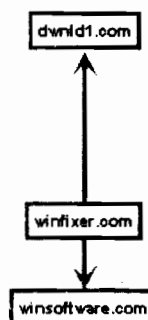
A few users

**McAfee SECURE Shopping**Your Secure Shopping Destination  
with Hundreds of Merchants[Shop Now >](#)

ALL SITES ARE

**AUTOMATED WEB SAFETY TESTING RESULTS FOR WINFIXER.COM****E-MAIL TESTS FOR WINFIXER.COM: ?****DOWNLOAD TESTS FOR WINFIXER.COM: ?****ONLINE AFFILIATIONS FOR WINFIXER.COM: ?****Linked to red sites**

When we tested this site we found links to winsoftware.com, which we found to be a distributor of downloads some people consider adware, spyware or other potentially unwanted programs.

**ANNOYANCES FROM WINFIXER.COM: ?****REVIEWER AND WEB SITE OWNER COMMENTS****USER REVIEW SUMMARY FOR WINFIXER.COM ?****Misleading site. [Reported]**

Feedback from some users indicated this site engaged in one or more negative or undesired activities.

This site is good (1)

This site spams (0)

Excessive popups (2)

Phishing or other scams (6)

**ATTACHMENT E****Page 252**

Adware, spyware, or viruses (94)

Bad shopping experience (6)

Browser exploit (16)



WINFIXER.COM WEB SITE OWNER COMMENTS (0) ?

Are you the owner of this site? Add a comment

USER REVIEWS (138) ?

page 1 of 14

Learn more about our reviewer system.

**Virus, try to download it. BAD**

Posted at 10/19/2008-12:34:46 PM by Zangosucks2. Reviewer View profile [ Reputation score: 1 - 9 ]

Rating: Adware, spyware, or viruses

**Rouge anti-spyware**

Posted at 10/03/2008-09:14:59 PM by Zangosucks2. Reviewer View profile [ Reputation score: 1 - 9 ]

**When I went to Winfixer.com, nothing happened.**

Posted at 09/15/2008-03:43:31 PM by virusflagger. Reviewer View profile [ Reputation score: 1 - 9 ]

Rating: Adware, spyware, or viruses

**This program fools people into believing there computer is infected. They pay money for rouge software, which then is downloaded and installs spyware and virus's onto the system!**

Posted at 08/26/2008-09:50:25 AM by Gooderz08. Reviewer View profile [ Reputation score: 0 - 9 ]

Rating: Adware, spyware, or viruses

**Reported on KTVU FOX 2, woman filed a lawsuit against the maker of the rogue software. You can see the report on YouTube. If this gets on your computer, don't pay these people. Use VundoFix, RogueRemover, MalwareByte's Anti-Malware, Spybot - Search and Destroy, or SuperAntiSpyware.**

Posted at 06/24/2008-10:42:16 PM by Jtaylor83. Reviewer View profile [ Reputation score: 1 - 9 ]

Rating: Adware, spyware, or viruses

**rogue software**

Posted at 07/04/2008-03:46:58 AM by Popop100. Reviewer View profile [ Reputation score: 0 - 9 ]

Rating: Adware, spyware, or viruses

**THIS IS A BAD SITE! STAY AWAY!!!!!! DON'T EVEN GO TO THE SITE!****It fooled our family. Someone downloaded it and it added a virus onto our computer.**

Posted at 07/02/2008-06:33:53 PM by webbieo. Reviewer View profile [ Reputation score: 1 - 9 ]

Rating: Adware, spyware, or viruses

Posted at 06/23/2008-04:44:16 PM by DsnapIntfirst. Reviewer View profile [ Reputation score: 0 - 9 ]

ATTACHMENT E

Page 253

Rating: Adware, spyware, or viruses

Adware. An enthusiast. An exorcist. A criminal.

If you want to help prevent adware, warn people about the dangers. Spread the word. If you find a virus, report it to a agency. If you know a criminal, report him. Save Our Computers.

If you want to know more about malware, there are sites out there that can teach you.

<http://sunbeltblog.blogspot.com/>

<http://lockergnome.com/>

<http://kasperskylabs.com/>

We can all put effort into this. If we can stop it, we will know how to stop all malware.

Help us!

Posted at 06/15/2008-07:56:32 PM by Protectzor. Reviewer View profile [ Reputation score: 1 - 9 ]

Rating: Adware, spyware, or viruses

This site is bad. There is spyware,virus,adware.com. And they try to scam you.

Posted at 05/29/2008-05:44:41 AM by [CFF5A08FFVIRUS. Reviewer View profile [ Reputation score: 1 - 9 ]

page 1 of 14

User Name

☐ Remember Me?

Password

Not a reviewer, yet? Register and leave a review of this site.

Get fully protected with McAfee Internet Security Suite.

Copyright © 2008 McAfee, Inc.

[Home](#) [Download](#) [Analysis](#) [Support](#) [About us](#) [Privacy policy](#) [Terms of service](#) [Site Owner Info](#) [Blog](#)

[Pick a language](#)

ATTACHMENT E

Page 254

McAfee SiteAdvisor™



HOME

DOWNLOAD

ANALYSIS

SUPPORT

BLOG

ABOUT US

Want to add your comments? Log in or Register

Look up a site report:

winsoftware.com



In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

Are you the owner of this site? Leave a comment

Contact information:

Country

Popularity



Canada



A few users

McAfee SECURE Shopping

Your Secure Shopping Destination  
with Hundreds of Merchants

Shop Now &gt;

ALL SITES ARE



## AUTOMATED WEB SAFETY TESTING RESULTS FOR WINSOFTWARE.COM

E-MAIL TESTS FOR WINSOFTWARE.COM: ?

DOWNLOAD TESTS FOR WINSOFTWARE.COM: ?

## 36 red downloads

In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

[View detailed analysis](#)

[Submit a download for analysis](#)

See how McAfee can protect your PC from dangerous downloads.

## Downloads we found on this site:

## Download

(WinAntiSpyware2007FreeInstall.exe)

EvidenceEraserPro 1.0 22.0 (EEPInstall...)

WinAntiSpyware 2006 (Unregistered versi...

WinAntiSpyware 2006 3.2.117.3 (WinAnti...

WinAntiSpyware 2006 Free 3.2.118.1 (Wi...

36 total downloads. See more.

## Analysis

Generic trojan

Winfixer trojan

Winfixer,BackDoor-BAC trojan

Winfixer

Winfixer

ONLINE AFFILIATIONS FOR WINSOFTWARE.COM: ?

## Linked to red sites

When we tested this site we found links to winantiviruspro.com, which we found to be a distributor of downloads some people consider adware, spyware or other potentially unwanted programs.



ANNOYANCES FROM WINSOFTWARE.COM: ?

REVIEWER AND WEB SITE OWNER COMMENTS

Page 255

ATTACHMENT E

## USER REVIEW SUMMARY FOR WINSOFTWARE.COM ?

**Negative behaviors. [Reported]**

Feedback from some users indicated this site engaged in one or more negative or undesired activities.

This site is good (0)

Excessive popups (2)

This site spams (1)

Phishing or other scams (0)

Adware, spyware, or viruses (34)

Bad shopping experience (1)

Browser exploit (0)



## WINSOFTWARE.COM WEB SITE OWNER COMMENTS (0) ?

Are you the owner of this site? Add a comment

## USER REVIEWS (43) ?

page 1 of 5

Learn more about our reviewer system.

Rating: Adware, spyware, or viruses

**Malware domain!**

**Typ: Rogue Software download**

This domain is used to spear "Rogue Software".

##### What is "Rogue Software"? #####

Rogue Software are computer applications which tries to trick you by telling you, that you are infected with spyware and/or viruses. But in truth you are just infected with this "Rogue Software". The malicious application tells you that the installed "Antivirus" or "Antispyware" application is just a demo version and that you have to buy the full version of the software to remove the virus / spyware from you computer. The truth is, that you are not infected. They just want to make money with your fear! Such malicious applications are also known as:

- Rogue Antivirus
- Rogue Software
- Rogue security software
- Rogue security application
- Fake security application

Normally the Rogue applicaiton changes your wallpaper and installs a fake bluescreen as screensaver (desktop hijacking).

Such "fake security applications" are promoted with many different names:

- AdwarePatrol
- AdwareRemover
- AntivirusXP 2008
- AntivirusXP 2009
- Antivirus 2009 Professional
- XP Security Center
- XP Antivirus 2009
- IE Defender
- WinFixer
- WinSpywareProtect
- Spyware Warrior
- Spyware Remover
- etc....

It's all the same crap! For more information take a look at  
[http://en.wikipedia.org/wiki/Rogue\\_software](http://en.wikipedia.org/wiki/Rogue_software)

##### Why is this software "Rogue"? #####

1. First of all the software don't ask you if you would like to install the applications - it just do it!
2. The malware says that you are infected with malware. Yeah, maybe thats true but the application DOESN'T remove the detected viruses from your machine!
3. The application fakes alert messages and bluescreens
4. They try to trap you by offering a "free spwayware/malware/virus" scan
5. There is a "Uninstall" button where you "can" uninstall the software. Well, when you press the

button the software just removes the uninstall button! The application still stays on you computer and shows you faked alert messages and bluescreens!

##### How to get infected #####

There are two different ways you can get infected which such malicious applications:

Normaly you get "infected" thru a malicious download (like in this case). But there are also well known malware which reloads such Rogue software after the infection (like wsnpoem / zbot do this). That's realy suspicious!

##### How to remove Rogue Software #####

Just download and install Malwarebytes "RogueRemover" from  
<http://www.malwarebytes.org/rogueremover.php> (The application is for free).

##### How to fight against malware #####

Submit Malware to MIRT: <http://www.castlecops.com/mirt>  
Download & install Spybot S&D: <http://www.safer-networking.org/en/download/>  
Download & Run McAfee Rootkit Detective: <http://vil.nai.com/VIL/STINGER/RKSTINGER.ASPX>  
Download & install Lavasoft Ad-Aware: [http://lavasoft.com/products/ad\\_aware\\_free.php](http://lavasoft.com/products/ad_aware_free.php)

Posted at 09/25/2008-09:50:37 AM by SaMsX, Experienced Reviewer, View profile [ Reputation score: 9 / 9 ]

Rating: Adware, spyware, or viruses

rogue software

Posted at 07/04/2008-03:47:20 AM by Popop100, Reviewer, View profile [ Reputation score: 0 / 9 ]

Rating: Adware, spyware, or viruses

Posted at 06/28/2008-05:47:27 PM by tetak, Reviewer, View profile [ Reputation score: 9 / 9 ]

Rating: Adware, spyware, or viruses

Adware. An enthusiast. An exorcist. A criminal.

If you want to help prevent adware, warn people about the dangers. Spread the word. If you find a virus, report it to a agency. If you know a criminal, report him. Save Our Computers.

if you want to know more about malware, there are sites out there that can teach you.

<http://sunbeltblog.blogspot.com/>  
<http://lockergnome.com/>  
<http://kasperskylabs.com/>

We can all put effort into this. If we can stop it, we will know how to stop all malware.

Help us!

Posted at 06/15/2008-07:57:03 PM by Protectzor, Reviewer, View profile [ Reputation score: 1 / 9 ]

Rating: Adware, spyware, or viruses

This website is a very dangerous one. I went to this site because I was tricked into it. It said "Win" in the beginning of their product name which I thought meant that it was something that was a part of Microsoft. Wrong. I started reading some of the reviews that "Fake Reviewers" wrote. It started saying that Norton and McAfee were bad and that those other products "Sucked" which lead me to believe that this site was bogus. No professional reviewer would use the word "Sucks" in their reviews. So I left the site but left it in my bookmarks so I could go back to it to observe it a little more later on. The next day when I went online, a whole bunch of ads started coming up to download some kind of spyware software like SpySheriff, WinFixer, WinAntivirus, and some others that were just words saying that there was a special software made for some trojan or virus called bloodhound or something like that. Freaky because it came up about every hour. Then some other ads that came up said that they were scanning my computer for viruses and then there were some that just came up saying "Would you like to scan for viruses?" Then there would be a Yes or No button or the X buttont to click. Anyone of those that you clicked, the website would still popup saying that they were scanning your computer. I tried scanning my computer for

any viruses or adware but nothing came up. But every once and a while, my antivirus would come up saying that there was adware on my computer and would ask me to scan my computer or not. After it found the adware, I tried to delete it but I couldn't because it would not allow me to. Don't go near this site or you will never be left alone. Don't be tricked.

Posted at 05/31/2008-06:17:03 AM by allyboo148, Reviewer . View profile [ Reputation score: 2 / 9 ]

Rating: Adware, spyware, or viruses

**This site is bad. There is spyware,adware,virus. And they trying to scam you.**

Posted at 05/29/2008-05:41:35 AM by [CFF5A08FFVIRUS, Reviewer . View profile [ Reputation score: 1 / 9 ]

Rating: Excessive popups

**Its all about that pop-up**

Posted at 05/06/2008-03:38:04 PM by Jumpstyle, Reviewer . View profile [ Reputation score: 0 / 9 ]

Rating: Adware, spyware, or viruses

**win-fixer is crap! it downloads adware and spyware without a warning! once i was just using the web,then a pop up comes up saying i have adware and i must scan as soon as possible instantly i knew it was fake so i clicked the x button,whats it doing now? it seems to be downloading it regardless! To save my pc,the only thing i could do is unplug my pc! if oyu see this crappy ad please do ctrl+alt+del,i also saw a piece of text saying you should click ctrl+F4 to close your browser!**

Posted at 04/20/2008-02:12:26 PM by jthome, Reviewer . View profile [ Reputation score: 1 / 9 ]

Rating: Adware, spyware, or viruses

**Part of WinFixer... not safe by any means.**

Posted at 04/03/2008-12:08:23 PM by Tom2405, Reviewer . View profile [ Reputation score: 1 / 9 ]

Rating: Excessive popups

**a pop up said download**

Posted at 12/30/2007-02:53:51 PM by jailbird46, Reviewer . View profile [ Reputation score: 1 / 9 ]

page 1 of 5

User Name

☐ Remember Me?

Password

Not a reviewer, yet? Register and leave a review of this site.

Get fully protected with McAfee Internet Security Suite.

StopBadware.org Report

[Click here to return to the reports page](#)

# Drive Cleaner 2006 (Free Version)

We find that Drive Cleaner 2006 (Free Version) is badware because it uses deceptive tactics to coerce users into installing the software and installs components that reportedly behave as adware without informing the user or seeking their consent. In addition, certain components automatically run in the background on startup without the user's knowledge or consent.



OVERALL RATING

**We currently recommend that users do not download the free version of Drive Cleaner 2006 that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

## Badware Behavior

Employs deceptive tactics to coerce the user into installing the software (Deceptive installation)

Installs adware (Deceptive installation)

Components of the software automatically run on startup (Interferes with computer use)

## REPORT INFORMATION

REPORT VERSION  
Version 1.0

DATE  
December 6, 2006

## Bad or Undisclosed Behavior

**Employs deceptive tactics to coerce the user into installing the software**

Drive Cleaner 2006 uses fear tactics to convince users to download their software. The free version of the software is usually advertised in pop-up ads. These pop-ups range from websites with flashing alerts that warn the user of "critical files" to webpages that masquerade as a Windows folder, complete with a fake dialog box asking the user if they want to "get rid of" critical files on their system. With the latter pop-ups, clicking "Yes" or "No" both redirect the user to a download page for Drive Cleaner 2006, thereby completely disregarding the user's response. Other pop-ups for Drive Cleaner 2006 demonstrate similar tactics. The text of these advertisements (many of which mimic legitimate system warnings), are almost uniformly alarmist and exaggerated. One advertisement is entitled "WARNING!!!!" and looks almost identical to a Windows' generated warning. According to this box, "Drive Cleaner found 948 dangerous files in your system." Other advertisements claim that the user has "compromising files" on their system that are being "tracked" by employers and government agencies that could potentially jeopardize the user's life. The number of "compromising files" that DriveCleaner claims to have "found" on the user's computer is always the arbitrary, but exorbitantly high number "948." The home page of the product further plays on users' fears by claiming that the files that have been discovered on the user's

## APPLICATION INFORMATION

### SELF-IDENTIFICATION

Drive Cleaner 2006 (Free Version) (also known as simply "DriveCleaner") identifies itself as a necessary software that will enable users to remove "critical files" that are being tracked on their computer. The feature page calls it "the latest released all drive cleaning software for Windows 98, WinNT, Win2000, WinMe & WinXP" and claims that "this program uses innovative technology developed by adult content treatment specialists, to scan your hard drive and eliminate every sign of prohibited material." The version we downloaded was labeled Version 1.0.37.0.

### PRODUCER

Drive Cleaner 2006 (Free Version) is produced by WinSoftware (<http://www.winsoftware.com>).

### OBTAINED

We obtained the Drive Cleaner 2006 application that we tested from <http://www.drivecleaner.com/> .freeware/

Attachment F

Page 259

computer "could compromise your career, your marriage or your overall status quo."

#### Installs adware

Drive Cleaner 2006 is reported to behave as adware mostly based on the aggressive tactics that it employs after installation to coerce users into buying the registered version of the product. Although we did not see visible advertisements and exaggerated alerts during our tests, the application is known to display threats constantly to coerce the user into purchasing the registered version. However, we did note that Drive Cleaner 2006 connects to an ad-server in the background during installation. The user is never made aware of these behaviors prior to or during installation.

#### Components of the software automatically run on startup

Installation of Drive Cleaner 2006 results in the addition of certain components to the startup menu, which means that these components run automatically in the background whenever Windows is started. Since Drive Cleaner 2006 itself did not actually work when we attempted to run it after installation, it is both interesting and suspicious that Drive Cleaner 2006 would have components that are running continuously without the user's knowledge. In essence, these processes could run forever in the background and the user would have no idea. Drive Cleaner 2006 never attempts to inform the user of this behavior nor seeks their consent before adding these entries to startup.

## Recommendations

---

**We recommend that the producers of the Drive Cleaner 2006 (Free Version) do the following:**

- Do not give users false and exaggerated threats about system vulnerability.
- Do not install adware without seeking the user's informed consent.
- Do not run components automatically on startup or in the background without the user's knowledge and consent.

**We currently recommend that users do not download the free version of Drive Cleaner 2006 that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

For more information, visit  
**[www.stopbadware.org](http://www.stopbadware.org).**

index.php?p=37&a=0&j=1&pp=1  
&w=1&ex=1&ap=1&hv=10  
&mpt=1164143824&ax=1&z=-  
5&link=4157&ad=swp\_dc\_us\_en\_  
ed1&aff=pp\_3158077922

#### BUNDLING

The version of Drive Cleaner 2006 that we tested is not bundled with other components.

StopBadware.org Report

[Click here to return to the reports page](#)

# PerformanceOptimizer

We find that PerformanceOptimizer (Trial Version) is badware because it installs deceptively, makes deceptive claims of system vulnerabilities in order to induce users to purchase the full version of the software, interferes with normal computer use by repeatedly prompting users to take previously declined actions, fails to inform users that the software will function as adware by prompting users to install additional software (including known badware), and fails to identify itself as the source of these advertisements.



OVERALL RATING

**We currently recommend that users do not install PerformanceOptimizer, unless the user is comfortable with the behaviors we have identified or until the application is updated to be consistent with the recommendations in this alert.**

## ALERT INFORMATION

ALERT DATE  
April 24, 2008

ALERT VERSION  
Version 1.0

PREVIOUS VERSIONS  
None

## BAD OR UNDISCLOSED BEHAVIOR

### Software installs deceptively (Guideline III.A)

The performanceoptimizer.com website attempts to silently download and install an ActiveX 'pre-installer' control for Internet Explorer. This pre-installer prompts the user to 'Continue' installing PerformanceOptimizer, although the user may not have chosen to download the pre-installer in the first place.

### Software does not clearly identify itself. (Guideline III.B)

The pop-up advertisements that PerformanceOptimizer displays on the user's computer are disguised as system alerts displayed by Microsoft Internet Explorer, and do not identify PerformanceOptimizer in any way as their source.

### Software does not fully, accurately, clearly, and conspicuously disclose the principal and significant features and functionality of the application prior to installation (Guideline II.A.a.iii)

The PerformanceOptimizer installer does not inform users that it will display frequent pop-up advertisements for additional software, both automatically and as a result of using PerformanceOptimizer's 'Update' feature. Some of the additional software promoted by PerformanceOptimizer has previously been reported as badware (WinAntiVirus).

### Software that interferes with the user's normal computer usage. (Guideline III.F)

PerformanceOptimizer reports exaggerated computer health threats in order to induce the user to purchase a registered version of the software which, it claims, will repair these problems. Some of these deceptive threats are delivered by frequent and sometimes difficult-to-dismiss pop-ups which interfere with the user's computer experience.

## APPLICATION INFORMATION

SOFTWARE VERSION  
Version 2.7 (build 2.26)

SELF-IDENTIFICATION  
"PerformanceOptimizer optimizes and compacts your registry for the best system performance!"

PRODUCER  
PerformanceOptimizer is a product of SellMoSoft, and is currently distributed at performanceoptimizer.com

OBTAINED  
PerformanceOptimizer was downloaded on 4/17/08 from a landing page on performanceoptimizer.com (link).

BUNDLING  
PerformanceOptimizer does not currently

appear to initially bundle additional software with the product, but frequently prompts users to install additional software distributed by SellMoSoft.

## Recommendations

---

**We recommend that SellMoSoft makes the following changes:**

- Stop distributing the PerformanceOptimizer 'Pre-installer' by silent, automatic download from the PerformanceOptimizer website.
- Inform users before they install the software that the application will repeatedly prompt the user to purchase a registered version of the software, and that it will display frequent pop-up alerts instructing the user to download additional software.
- Stop reporting exaggerated system vulnerabilities to users, to induce them to install or purchase the product or other products.
- Conspicuously attribute all of the software's behaviors, including pop-up alerts, to PerformanceOptimizer.

**We currently recommend that users do not install PerformanceOptimizer, unless the user is comfortable with the behaviors we have identified or until the application is updated to be consistent with the recommendations in this alert.**

**This alert represents StopBadware's findings during our initial testing period. Additional badware behaviors that were not initially detected may exist in the application.**

For more information, visit  
**[www.stopbadware.org](http://www.stopbadware.org).**

StopBadware.org Report

[Click here to return to the reports page](#)

# WinAntiSpyware 2006 (Unregistered Version)

We find that WinAntiSpyware 2006 (Unregistered Version) is badware because it makes exaggerated claims of system vulnerability in order to encourage the user to purchase the full version. In essence, WinAntiSpyware 2006 (Unregistered Version) belongs to that subset of badware that is often termed "nagware" or "extortionware" -- that is, software that exists solely to encourage (generally through deceptive or annoying means) users to upgrade to a full version of the product. In addition, WinAntiSpyware 2006 (Unregistered Version) does not disclose to the user that the program will run automatically at start-up, continuously run a process in the background, or download updates without user consent.



OVERALL RATING

**We currently recommend that users do not install the version of WinAntiSpyware that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**



## Badware Behavior

Displays pop-up ads and makes distracting auditory alerts  
(Interferes with computer use)

Makes exaggerated claims of system vulnerability  
(Deceptive functionality)

Downloads automatic updates without user's consent  
(Deceptive installation)

Automatically runs on startup (Interferes with computer use  
without disclosure)

## Bad or Undisclosed Behavior

**Displays pop-up ads and makes distracting auditory alerts**

Approximately every ten to twenty minutes, WinAntiSpyware 2006 (Unregistered Version) displays "WinAntiSpyware 2006 (Unregistered Version) Alert" pop-ups that are essentially advertisements for the full

ATTACHMENT F

Page 263

## REPORT INFORMATION

REPORT VERSION  
1.0

DATE  
09/27/2006

## APPLICATION INFORMATION

### SELF-IDENTIFICATION

WinAntiSpyware 2006 identifies itself as an application that enables users to get rid of spyware and adware from their computer. According to its website, it claims to be the "best integral Spyware protection" and "ultimate Spyware protection solution."

### PRODUCER

WinAntiSpyware 2006 (Unregistered Version) is produced by WinSoftware, Inc. (<http://www.winsoftware.com/>). The winsoftware.com domain is registered in Peterborough, ON, Canada.

version of WinAntiSpyware 2006. These pop-up warnings open in separate windows and some of them make siren noises, thereby disrupting the user's ability to use their computer. WinAntiSpyware 2006 (Unregistered Version) does not inform users during installation that it will display these pop-up alarms.

#### **Makes exaggerated claims of system vulnerability**

WinAntiSpyware 2006 (Unregistered Version) uses alarmist language and deceptive tactics to scare users into upgrading to the full version of its software. The software claims "Spyware detected!" and "Spyware infection found!", and warns of "critical SPYWARE objects" over a few tracking cookies that are considered to be harmless. Additional warnings shown after a system scan state that "The threats found on your computer are very likely to create further problems if not fixed immediately, such as: Aggressive advertising popups; Slow web page loading and browser crashes; Hackers can steal your Credit Card details; Violate your privacy during Web surfing; Your local and online passwords stolen." The sense of exaggeration is heightened by the audio alarm associated with the alerts. In order to "clean" the computer, the user must register WinAntiSpyware 2006, which entails purchasing the full version of the software.

#### **Downloads updates without user's consent**

WinAntiSpyware 2006 (Unregistered Version) automatically downloads updates regularly on the user's computer without the user's consent. This automatic updating is not disclosed to the user at any time -- whether during the initial installation of WinAntiSpyware 2006 or as the individual updates occur. There is also no option given to the user to stop these updates from happening. The user is given no information on what these updates are or what purpose they serve.

#### **Automatically runs on startup**

WinAntiSpyware 2006 (Unregistered Version) automatically runs in the systems tray on startup. The application does not inform users that it will run on startup, and has no setting to allow users to disable this function.

## **Recommendations**

---

#### **We recommend that the producers of WinAntiSpyware 2006 (Unregistered Version) do the following:**

- Stop making exaggerated claims of system vulnerability.
- Disclose to the user during installation that WinAntiSpyware 2006 (Unregistered Version) will be launching periodic pop-ups and auditory alarms and make it clear how frequent those alarms will be.
- Inform the user during installation that WinAntiSpyware 2006 will automatically run on startup, or provide the user with the option not to run the software on startup.
- Clearly disclose to the user when updates are available and ask for their consent before continuing with the update.

**We currently recommend that users do not install the version of WinAntiSpyware 2006 that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

For more information, visit  
[www.stopbadware.org](http://www.stopbadware.org).

#### **OBTAINED**

We obtained WinAntiSpyware 2006 (Unregistered Version) from <http://www.winantispyware.com/download/2006/index.php>.

#### **BUNDLING**

The version of WinAntiSpyware 2006 we downloaded is not bundled with any other products.

StopBadware.org Report

[Click here to return to the reports page](#)

# WinAntiVirus 2006

We find that WinAntiVirus 2006 (Unregistered Version) is badware because it makes exaggerated claims of system vulnerability in order to encourage the user to purchase the full version. In essence, WinAntiVirus 2006 (Unregistered Version) belongs to that subset of badware that is often termed "nagware" or "extortionware" -- that is, software that exists solely to encourage (generally through deceptive or annoying means) users to upgrade to a full version of the product. In addition, WinAntiVirus 2006 (Unregistered Version) automatically disables Windows Firewall without notifying to the user. It also fails to disclose to the user that the program will run automatically at start-up, continuously run a process in the background, or download updates without user consent.



OVERALL RATING

**We currently recommend that users do not install the version of WinAntiVirus 2006 that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**



## Badware Behavior

Disables Windows Firewall (Modifies other software without disclosure)

Makes exaggerated claims of system vulnerability (Deceptive functionality)

Downloads automatic updates without user's consent (Deceptive installation)

Continuously runs a process in the background (Interferes with computer use without disclosure)

Automatically runs on startup (Interferes with computer use without disclosure)

## REPORT INFORMATION

REPORT VERSION  
1.0

DATE  
9/27/2006

## APPLICATION INFORMATION

### SELF-IDENTIFICATION

WinAntiVirus 2006 identifies itself as an application that "helps block, detect and eliminate viruses and Trojans, safeguarding your computer from security threats that are constantly growing in number and complexity."

### PRODUCER

WinAntiVirus 2006 (Unregistered Version) is produced by WinSoftware, Inc. (<http://www.winsoftware.com/>). The winsoftware.com domain is registered in Peterborough, ON, Canada.

### OBTAINED

We obtained WinAntiVirus 2006

ATTACHMENT F

Page 265

## Bad or Undisclosed Behavior

### Disables Windows Firewall

WinAntiVirus 2006 (Unregistered Version) automatically disables Windows Firewall during the installation process. The disabling of Windows Firewall is not disclosed to the user at any point, nor does WinAntiVirus give any reasons for their actions. By disabling the user's firewall, WinAntiVirus may leave the user's computer more vulnerable to viruses and other badware.

(Unregistered Version) from <http://winantivirus.com/pages/scanner/index.php>.

#### **Makes exaggerated claims of system vulnerability**

WinAntiVirus 2006 (Unregistered Version) uses alarmist language and deceptive tactics to scare users into upgrading to the full version of its software. The software claims "Severe Infections detected!" over a few tracking cookies that are considered to be harmless. Additional warnings shown after a system scan state that "The threats found on your computer are very likely to create further problems if not fixed immediately, such as: Lost Documents and Settings; Permanent Data Loss; System not starting up; System slowdown and crashes; Loss of Internet Connection; Infecting other computers on your network." In order to "clean" the computer, the user must register WinAntiSpyware 2006, which entails purchasing the full version of the software.

#### **BUNDLING**

The version of WinAntiVirus 2006 we downloaded was not bundled with any other products.

#### **Continuously runs a process in the background**

A process named FWSvc.exe runs continuously in the background of the user's machine, even after the user has exited WinAntiVirus 2006. The software fails to disclose that this process will always be running in the background. In fact, the user would not be aware of this behavior unless they looked at the running processes on Windows Task Manager. Information available online on the process identifies it as malware and potentially harmful to the user's computer.

#### **Downloads updates without user's consent**

WinAntiVirus 2006 (Unregistered Version) automatically downloads "spyware database updates" and "application updates" on the user's computer without the user's consent. This automatic updating is not disclosed to the user at any time -- whether during the initial installation of WinAntiVirus 2006 or as the individual updates occur. There is also no option given to the user to stop these updates from happening. The user is given no information on what these updates are or what purpose they serve.

#### **Automatically runs on startup**

WinAntiVirus 2006 (Unregistered Version) automatically runs in the systems tray on startup. The application does not inform users that it will run on startup, and has no setting to allow users to disable this function.

## **Recommendations**

---

#### **We recommend that the producers of WinAntiVirus 2006 (Unregistered Version) do the following:**

- Do not disable Windows Firewall or any other software without clearly disclosing to the user what modifications will be made, why they are necessary, and seeking the user's informed consent.
- Stop making exaggerated claims of system vulnerability.
- Inform the user during installation that WinAntiVirus 2006 will automatically run on startup, or provide the user with the option not to run the software on startup.
- Disclose to the user that WinAntiVirus 2006 (Unregistered Version) will run a process in the background and clearly disclose the reasons why the process needs to run constantly, even when WinAntiVirus 2006 (Unregistered Version) is not running.
- Clearly disclose to the user when updates are available and ask for their consent before continuing with the update.

**We currently recommend that users do not install the version of WinAntiVirus 2006 that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

ATTACHMENT F

Page 266

For more information, visit  
**[www.stopbadware.org](http://www.stopbadware.org)**.

StopBadware.org Report

[Click here to return to the reports page](#)

# WinFixer 2005, WinFixer 2006

We find that WinFixer 2005 and WinFixer 2006 are badware because they do not provide users with their licensing agreements during installation, they make exaggerated claims of "severe system threats" to the user's computer, and do not disclose that they will automatically launch whenever the user starts Windows. In addition, WinFixer 2005 installs a possible rootkit.



OVERALL RATING

**We currently recommend that users do not install the version of WinFixer that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

## Badware Behavior

No license agreement or prompts during installation  
(Deceptive Installation)

Contains a possible rootkit (Deceptive Identification)

Makes exaggerated claims of "Severe System Threats" (Deceptive Functionality)

Launches automatically after reboot and scans computer  
(Interferes with Computer Use)

## Bad or Undisclosed Behavior

### No license agreement or prompts during installation

Adequate disclosure of user rights should be made in the license agreement and also in a clear human readable fashion during the install process. Licenses are terms can be found on the producer's website but not at all during the installation process. This becomes especially troublesome when WinFixer is downloaded from a third party.

### Contains a possible rootkit

The 2005 version of WinFixer contains a component, df\_kmd.sys, which several badware analysis websites label as a rootkit, or parasite. Rootkits may be being used to disguise an application from detection, making it difficult for a user to remove it.

### Makes exaggerated claims of "Severe System Threats"

During a typical first installation, WinFixer claimed to find roughly one thousand "Severe System Threats," even though it was scanning a brand-new installation of Windows. Based on information provided by

## REPORT INFORMATION

REPORT VERSION  
Version 1.0

DATE  
May 23, 2006

## APPLICATION INFORMATION

### SELF-IDENTIFICATION

WinFixer's full name is "WinFixer," followed by a version year of 2005 or 2006. It advertises itself as "the ultimate solution that safeguards your system by cleaning the Windows registry, fixing damaged files, running disk cleanup and detecting hard drive errors. Winfixer protects your system against potential damages and problems, ensuring its optimal performance."

### PRODUCER

winfixer.com does not publish any information about the producers of WinFixer. The winfixer.com domain is registered in Kiev, Ukraine.

### OBTAINED

We obtained WinFixer 2005 from <http://download.winfixer.com/files/Trial/2523/WinFixer2005TrialSetup.exe> and WinFixer 2006 from <http://download.winfixer.com/files/WinFixer2006FreeSetup.exe>.

BUNDLING

Page 268

ATTACHMENT F

The version of WinFixer we downloaded from the above URL is not bundled with other software.

the application, it seems unlikely that most of these "severe system threats" were actually severe system threats, and it is possible that WinFixer greatly exaggerated the scope of the problem in order to increase sales of the full version of its application.

WinFixer 2005 actually provided some information on which files and components it considered severe threats. These included components that were benign (such as temporary internet files and cookies) or even beneficial. For example, WinFixer 2005 claimed that registry keys related to a legitimate research and debugging tool (HijackThis) were "spyware" and marked them as a "critical system threat." While we realize that all such claims are subjective and open to discussion, it seems likely that HijackThis was targetted because HijackThis is often used to diagnose and remove WinFixer. WinFixer 2006 no longer provides any information to the user about the nature of the "severe threats" on their computer, so it is impossible to tell whether any of the claimed threats are valid.

The same WinFixer screen that tells users that they have numerous "Severe System Threats" (or errors) also warns them that if they do not fix the system immediately the errors will "very likely create further problems" such as "lost documents and profile settings," "physical data loss," "system not starting up," and "system slowdowns, crashes and freezes." With WinFixer 2006, this screen appears not only when users start Windows or run WinFixer, but also when they attempt to shut down or restart their computer. In this latter case, WinFixer 2006 displays a dialog box stating that "shutdown is NOT recommended" due to numerous "severe system errors." According to WinFixer 2006, shutting down the computer "while it has errors in the registry database or file system ... is very likely [to cause] further problems." Since the test systems we installed WinFixer on were clean, non-badware-infected test profiles, these claims are highly unlikely.

#### **Launches automatically after reboot and scans computer**

The application does not disclose to the user that WinFixer will run each time at startup. This means that each time the user restarts her computer, a screen will pop up claiming to have identified a variety of "severe system threats" and urging her to purchase the complete version of WinFixer. Moreover, WinFixer 2006 also runs whenever the user attempts to shut down or restart her computer, warning her that shutting down the computer is "very likely" to result in further problems. These actions will continue to occur unless the user disables this option or, in the case of the shutdown pop-up, unless the user exits WinFixer 2006 in the system tray.

## **Recommendations**

---

#### **We recommend that WinFixer do the following:**

- Provide licensing agreements to users during installation and disclose that WinFixer will automatically launch when Windows restarts and, in the case of WinFixer 2006, at shutdown.
- Do not exaggerate claims of "severe system threats" by flagging benign or beneficial files or components.
- Do not install rootkits or any other form of malicious software.

**We currently recommend that users do not install the version of WinFixer that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

For more information, visit

Page 269

ATTACHMENT F

**www.stopbadware.org.**

StopBadware.org Report

[Click here to return to the reports page](#)

# XP Antivirus 2008

We find that XP Antivirus 2008 (Unregistered Version) is badware because it makes deceptive claims of system vulnerabilities in order to induce users to purchase the full version of the software, because it interferes with normal computer use by automatically running a background process which repeatedly prompts the user to take a previously declined action, and because the software cannot be uninstalled using the Windows Add/Remove Programs tool, or without downloading an additional uninstaller.



OVERALL RATING

**We currently recommend that users do not install the versions of XP AntiVirus 2008 that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated to be consistent with the recommendations in this report.**

## BAD OR UNDISCLOSED BEHAVIOR

### **Software does not identify the entity responsible for the software (Guideline II.A.a.ii)**

XP Antivirus 2008 does not inform the user at any time that it is a product of INNOVAGEST 2000 S.L. (<http://innovagest2000.com>)

### **Software does not fully, accurately, clearly, and conspicuously disclose the principal and significant features and functionality of the application prior to installation (Guideline II.A.a.iii)**

The XP Antivirus 2008 installer does not inform users that it will register the application to load a continuous background process at startup, which will repeatedly report exaggerated security threats to the user in order to persuade the user to purchase the software.

### **Software uses deceptive behavior that would force the average user to take an action they would otherwise decline. (Guideline III.F)**

XP Antivirus reports exaggerated security threats to induce the user to purchase a registered version of the software which, it claims, will remove these infections. In fact, many of these reported security threats (eg. Spyware.IMMonitor, Zlob.PornAdvertiser.ba, Infostealer.Banker.E) were not present on our testing computer, and registering the software appeared to simply cause the next scan to report that the computer was clean, even if we never actually ran the XP Antivirus 2008 'remove infections' process.

### **Software is not easy to uninstall completely, because it fails to use the system uninstall tools, or requires the download of an additional uninstallation tool. (Guideline III.G.2)**

XP Antivirus 2008 cannot be uninstalled using the Windows Add/Remove Programs tool. The uninstall tool that is bundled with the software failed to remove the program in one of the two publicly-released builds of XP Antivirus that we tested, and the online 'help' document for both builds instructs users to download a separate uninstallation tool to remove the software.

## REPORT INFORMATION

REPORT DATE  
March 20, 2008

REPORT VERSION  
Version 1.0

PREVIOUS VERSIONS  
None

## APPLICATION INFORMATION

SOFTWARE VERSION  
Builds of XP Antivirus 2008 were downloaded on 3/17/08 from [xpantivirus2008.com](http://xpantivirus2008.com), and on 3/18/08 from [xpantivirus.com](http://xpantivirus.com)

SELF-IDENTIFICATION  
From the XP Antivirus 2008 installer:  
"This program will download and install XP Antivirus 2008 on your computer."

PRODUCER  
XP Antivirus 2008 is a product of Innovagest 2000, and is currently distributed at [xpantivirus.com](http://xpantivirus.com)

OBTAINED  
We obtained two builds of XP Antivirus 2008 - one from [xpantivirus2008.com](http://xpantivirus2008.com)

ATTACHMENT F

Page 271

## Recommendations

---

**We recommend that INNOVAGEST 2000 S.L. makes the following changes:**

- Inform users at the time that XP Antivirus 2008 is installed that the application is a product of Innovagest 2000.
- Inform users before they install the software that the application will automatically and continuously run a background process on the computer which repeatedly prompts the user to purchase a registered version of the software, or allow users to set the program to not load at startup.
- Stop reporting exaggerated system vulnerabilities to users, to induce them to purchase the product.
- Ensure that the software can be clearly identified and completely removed using system uninstallation tools, such as Windows' Add/Remove Programs tool.

**We currently recommend that users do not install the versions of XP Antivirus 2008 that we tested, unless the user is comfortable with the software behaviors we identify or until the application is updated to be consistent with the recommendations in this report.**

**This alert represents StopBadware's findings during our initial testing period. Additional badware behaviors that were not initially detected may exist in the application.**

For more information, visit  
**[www.stopbadware.org](http://www.stopbadware.org).**

which was downloaded on 3/17/08 and which now appears to be unavailable, and one from xpantivirus.com which was downloaded on 3/18/08 and which continues to be available from that source.

### **BUNDLING**

XP Antivirus 2008 does not currently appear to bundle additional software with the product.

Web Images Maps News Shopping Gmail more ▼

Sign in

Google

drivecleaner.com

Search

Advanced Search  
Preferences

Web

Results 1 - 10 of about 45,200 for [drivecleaner.com](http://drivecleaner.com). (0.11 seconds)**DriveCleaner - Home**

This site may harm your computer.

**DriveCleaner** eliminates them all! Simply deleting these files is not enough. **DriveCleaner** really gets rid of the evidence! ...[www.drivecleaner.com/](http://www.drivecleaner.com/) - Similar pages**Drivecleaner.com has pop up that tells me my computer has gay ...**history on computer can not be checked as it was o...  
[answers.yahoo.com/question/index?](http://answers.yahoo.com/question/index?qid=20060711135803AA6chmE)

qid=20060711135803AA6chmE - 55k -

Cached - Similar pages

**Drivecleaner.com Pest - Tech Support Guy Forums**

15 posts - Last post: Dec 6, 2006

There is a redirect that shows up when I click on a link on my IE homepage and it goes to: ...

[forums.techguy.org/malware-removal-hijackthis-logs/521442-drivecleaner-com-pest.html](http://forums.techguy.org/malware-removal-hijackthis-logs/521442-drivecleaner-com-pest.html) - 178k -

Cached - Similar pages

**[drivecleaner.com/freeware..](http://drivecleaner.com/freeware..) HORRIBLE POP UPS - Tech Support Guy ...**

11 posts - Last post: Jun 29, 2007

HELP WITH :

<http://drivecleaner.com/freeware/in...ax=1&ed=1&ex=1>

nASTY POP UPS. I CANT SEEM TO GET RID OF THEIS THROUGH SPYWARE, ADAWARE, ...

[forums.techguy.org/malware-removal-hijackthis-logs/589333-drivecleaner-com-freeware-horrible-pop.html](http://forums.techguy.org/malware-removal-hijackthis-logs/589333-drivecleaner-com-freeware-horrible-pop.html) - 132k -

Cached - Similar pages

More results from [forums.techguy.org](http://forums.techguy.org) »**What is drivecleaner.com? - Mac Forums**

3 posts - Last post: Aug 18, 2007

Uhhh I just clicked something, I think on Digg.com, and something for [drivecleaner.com](http://drivecleaner.com) popped up..... do I need to do this scan? ...[forums.macrumors.com/showthread.php?t=337544](http://forums.macrumors.com/showthread.php?t=337544) - 45k - Cached - Similar pages**Amazon.com: drivecleaner.com/: Website Details****Drivecleaner** - Do the internet a favour and LEAVE US ALONE! ... 1.0 out of 5 stars**drivecleaner.com** are losers, September 1, 2007 ...[www.amazon.com/drivecleaner-com/dp/B000G5RIWW](http://www.amazon.com/drivecleaner-com/dp/B000G5RIWW) - 143k - Cached - Similar pages**[www.drivecleaner.com](http://www.drivecleaner.com)****Drivecleaner** for a Clean System **Drivecleaner.com** is the official site of the software called **Drivecleaner**. The software claims to cleanse your system of all ...[hubpages.com/hub/wwwdrivecleanercom](http://hubpages.com/hub/wwwdrivecleanercom) - 19k - Cached - Similar pages**Drivecleaner.com - Eliminate All Evidence | Visit Driveclean...**

Whether you like it or not, pornography is flooding the Internet since its beginnings. Even if it isn't by your own choice, sooner or later you will land o .

## Sponsored Links

**Don't Get DriveCleaner**

Until You DriveCleaner Reviews.

Free Download. 100% Guaranteed.

[www.ConsumerSoftwareReviews.com](http://www.ConsumerSoftwareReviews.com)**Drive Cleaner Removal Now**

Remove Drive Cleaner Virus Now

5 Stars - Download 100% Free!

[AdwareAlert.com/Drive-Cleaner](http://AdwareAlert.com/Drive-Cleaner)**DriveCleaner Exposed?**

Don't buy antispware

until you read this

[spywarefool.blogspot.com](http://spywarefool.blogspot.com)**Caught out with porn?**

Detect adult files on your computer

Clean up hard drive porn easily

[www.hyperdynesoftware.com](http://www.hyperdynesoftware.com)**Remove DriveCleaner.**

How to Remove DriveCleaner.

DriveCleaner Removal Instructions.

[www.removal-instructions.com](http://www.removal-instructions.com)**DriveCleaner 2007 Removal**

DriveCleaner 2007 Removal Guide.

Remove DriveCleaner 2007 easy way.

[hubpages.com/hub/DriveCleaner](http://hubpages.com/hub/DriveCleaner)

www.killerstartups.com/Web-App-Tools/drivecleaner.com-eliminate-all-evidence - 68k -  
Cached - Similar pages

Win32/Beenut Family - CA

Jul 24, 2006 ... If the user clicks on the "OK" button, the trojan downloads **DriveCleaner** from  
the domain go.**drivecleaner.com**. ...

www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=57168 - 59k - Cached - Similar pages

**Drivecleaner.com = spyware site - news.admin.net-abuse.email ...**

18 posts - 15 authors - Last post: Jun 18, 2007

**Drivecleaner.com** opened a window in my browser without my authorization, or without my  
even attempting to access the site. ...

groups.google.com/group/news.admin.net-abuse.email/browse\_thread/thread/  
89dfa2805abb7a42/1c58f0996fc9a1d5 - 202k - Cached - Similar pages

1 2 3 4 5 6 7 8 9 10 **Next**

---

drivecleaner.com

Search

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied?](#) [Help us improve](#) |  
[Try Google Experimental](#)

---

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [Privacy](#) - [About Google](#)

Welcome **sdrexler** Logout My Account

[Whois >](#) | [Domain Suggestions >](#) | [For Sale >](#) | [Auctions >](#) | [Advanced Auctions >](#) | [Domain Search >](#) | [Domain Monitor >](#)  
[Domain Directory](#) | [Ping >](#) | [Traceroute >](#) | [My IP Address](#) | [Cheap Domain Name Registration](#) | [Bulk Check](#) | [more >](#)  
**Power Tools:** | [Reverse IP](#) | [Domain History](#) | [Mark Alert](#) | [Name Server Spy](#) | [Domain Typo New](#) | [XML API](#)

## Reverse-IP

### Search Again

Enter the IP address or hostname of a webserver

IP Address/Hostname: winsoftware.com

IP Search

Reverse-IP lookups today: 1/1,000

### Search Results for 66.244.254.46 [reverse DNS - box46.yyz1.setupahost.net]

24 Results for 66.244.254.46 (Winsoftware.com)

| Website                                  | DMOZ       | Wikipedia         | Yahoo      |
|------------------------------------------|------------|-------------------|------------|
| 1. <a href="#">Betbonus.com</a>          | 0 listings | 0 listings        | 0 listings |
| 2. <a href="#">Billingintegrator.com</a> | 0 listings | 0 listings        | 0 listings |
| 3. <a href="#">Completebilling.com</a>   | 0 listings | 0 listings        | 0 listings |
| 4. <a href="#">Driveprotector.com</a>    | 0 listings | 0 listings        | 0 listings |
| 5. <a href="#">Eglobalbilling.com</a>    | 0 listings | 0 listings        | 0 listings |
| 6. <a href="#">Extrabilling.com</a>      | 0 listings | 0 listings        | 0 listings |
| 7. <a href="#">Multimediafixer.com</a>   | 0 listings | 0 listings        | 0 listings |
| 8. <a href="#">Openbillsolutions.com</a> | 0 listings | 0 listings        | 0 listings |
| 9. <a href="#">Realtimenetbill.com</a>   | 0 listings | 0 listings        | 0 listings |
| 10. <a href="#">Smileydistrict.com</a>   | 0 listings | 0 listings        | 0 listings |
| 11. <a href="#">Vantagesoftware.com</a>  | 0 listings | 0 listings        | 0 listings |
| 12. <a href="#">Webinvestigator.com</a>  | 0 listings | 0 listings        | 0 listings |
| 13. <a href="#">Winadblocker.com</a>     | 0 listings | 0 listings        | 0 listings |
| 14. <a href="#">Winantispam.com</a>      | 0 listings | 0 listings        | 0 listings |
| 15. <a href="#">Winantispy.com</a>       | 0 listings | 0 listings        | 0 listings |
| 16. <a href="#">Wincontentfilter.com</a> | 0 listings | 0 listings        | 0 listings |
| 17. <a href="#">Windrivecleaner.com</a>  | 0 listings | 0 listings        | 0 listings |
| 18. <a href="#">Windrivesafe.com</a>     | 0 listings | 0 listings        | 0 listings |
| 19. <a href="#">Winfirewall.com</a>      | 0 listings | 0 listings        | 0 listings |
| 20. <a href="#">Winnanny.com</a>         | 0 listings | 0 listings        | 0 listings |
| 21. <a href="#">Winpopupguard.com</a>    | 0 listings | 0 listings        | 0 listings |
| 22. <a href="#">Winprivacyguard.com</a>  | 0 listings | 0 listings        | 0 listings |
| 23. <a href="#">Winproductions.com</a>   | 0 listings | 0 listings        | 0 listings |
| 24. <a href="#">Winsoftware.com</a>      | 0 listings | <u>1 listings</u> | 0 listings |


[Members Area](#) | [Hosting Metrics](#) | [Stock Ticker](#) | [Download](#) | [Domain Registration](#) | [Whois](#) | [Domain Suggestions](#) | [Site Map](#)



## Reverse-IP

Search Again

IP Address/Hostname: **billingnow.com**

IP Search

Examples: 127.% or 127.0.0.1 - Reverse-IP lookups today: 5/1,000

## Other Server

The domain name Billingnow.com has more than one server hosting its domains. You can select a different server below.

| IP Address    | Domains |
|---------------|---------|
| 66.244.254.63 | 49      |
| 66.244.254.64 | 1       |

## Search Results for 66.244.254.63 [reverse DNS - rr-grp1.yyz1.cl1.setupahost.net]

## 49 Results for 66.244.254.63 (Billingnow.com)

|                                           |            |            |            |
|-------------------------------------------|------------|------------|------------|
| 1. <a href="#">Adsmmediabroker.com</a>    | 0 listings | 0 listings | 0 listings |
| 2. <a href="#">Ahctravels.com</a>         | 0 listings | 0 listings | 0 listings |
| 3. <a href="#">Air-deals.net</a>          | 0 listings | 0 listings | 0 listings |
| 4. <a href="#">Airhotelcars.com</a>       | 0 listings | 0 listings | 0 listings |
| 5. <a href="#">Amxtravel.com</a>          | 0 listings | 0 listings | 0 listings |
| 6. <a href="#">Antivirusproshop.com</a>   | 0 listings | 0 listings | 0 listings |
| 7. <a href="#">Billingcomplete.com</a>    | 0 listings | 0 listings | 0 listings |
| 8. <a href="#">Billingnow.com</a>         | 0 listings | 0 listings | 0 listings |
| 9. <a href="#">Bookmyfares.com</a>        | 0 listings | 0 listings | 0 listings |
| 10. <a href="#">Drivecleaner.com</a>      | 0 listings | 0 listings | 0 listings |
| 11. <a href="#">Enhanceyourbust.com</a>   | 0 listings | 0 listings | 0 listings |
| 12. <a href="#">Errorprotector.com</a>    | 0 listings | 0 listings | 0 listings |
| 13. <a href="#">Errorsafe.com</a>         | 0 listings | 0 listings | 0 listings |
| 14. <a href="#">Herbalgeneration.com</a>  | 0 listings | 0 listings | 0 listings |
| 15. <a href="#">Incrediseek.com</a>       | 0 listings | 0 listings | 0 listings |
| 16. <a href="#">Intrudertrace.com</a>     | 0 listings | 0 listings | 0 listings |
| 17. <a href="#">Ipodpremium.com</a>       | 0 listings | 0 listings | 0 listings |
| 18. <a href="#">Kazaa-update.com</a>      | 0 listings | 0 listings | 0 listings |
| 19. <a href="#">Kpremium.com</a>          | 0 listings | 0 listings | 0 listings |
| 20. <a href="#">Maxfares.com</a>          | 0 listings | 0 listings | 0 listings |
| 21. <a href="#">Mediaopp.com</a>          | 0 listings | 0 listings | 0 listings |
| 22. <a href="#">Nortoncomparison.com</a>  | 0 listings | 0 listings | 0 listings |
| 23. <a href="#">Onestoponlineshop.net</a> | 0 listings | 0 listings | 0 listings |
| 24. <a href="#">Pcturbopro.com</a>        | 0 listings | 0 listings | 0 listings |
| 25. <a href="#">Personalantispy.com</a>   | 0 listings | 0 listings | 0 listings |
| 26. <a href="#">Popupavenger.com</a>      | 0 listings | 0 listings | 0 listings |
| 27. <a href="#">Popupguard.com</a>        | 0 listings | 0 listings | 0 listings |
| 28. <a href="#">Privacyprotector.com</a>  | 0 listings | 0 listings | 0 listings |
| 29. <a href="#">Pro-antivirus-spy.com</a> | 0 listings | 0 listings | 0 listings |
| 30. <a href="#">Redirect0897896.com</a>   | 0 listings | 0 listings | 0 listings |
| 31. <a href="#">Sagentgroup.com</a>       | 0 listings | 0 listings | 0 listings |

|                             |                   |                   |                   |
|-----------------------------|-------------------|-------------------|-------------------|
| 32. Search42.com            | 0 listings        | 0 listings        | 0 listings        |
| 33. Searchfindsearch.com    | 0 listings        | 0 listings        | 0 listings        |
| 34. Setupahost.net          | 0 listings        | 0 listings        | 0 listings        |
| 35. Smax.us                 | 0 listings        | 0 listings        | 0 listings        |
| 36. Sysprotect.com          | 0 listings        | 0 listings        | 0 listings        |
| 37. Systemdoctor.com        | 0 listings        | 0 listings        | 0 listings        |
| 38. Verioproducts.com       | 0 listings        | 0 listings        | 0 listings        |
| 39. Versatasoftware.com     | 0 listings        | 0 listings        | 0 listings        |
| 40. Viadorgroup.com         | 0 listings        | 0 listings        | 0 listings        |
| 41. Vipfares.com            | 0 listings        | 0 listings        | 0 listings        |
| 42. Virusguard.com          | 0 listings        | 0 listings        | 0 listings        |
| 43. Virussoftwarereview.com | 0 listings        | 0 listings        | 0 listings        |
| 44. Virussw.com             | 0 listings        | 0 listings        | 0 listings        |
| 45. Winantispyware.com      | 0 listings        | <u>1 listings</u> | 0 listings        |
| 46. Winantivirus.com        | <u>1 listings</u> | 0 listings        | <u>1 listings</u> |
| 47. Winantiviruspro.com     | 0 listings        | 0 listings        | 0 listings        |
| 48. Winnanny.com            | 0 listings        | 0 listings        | 0 listings        |
| 49. Winpluspak.com          | 0 listings        | 0 listings        | 0 listings        |



## Reverse-IP

Search Again

IP Address/Hostname: advancedcleaner.com

Examples: 127.0.0.1 or 127.0.0.1 - Reverse-IP lookups today: 1/1,000

## Other Server

The domain name Advancedcleaner.com has more than one server hosting its domains. You can select a different server below.

| IP Address     | Domains |
|----------------|---------|
| 83.170.116.39  | 5       |
| 93.190.139.197 | 9       |

## Search Results for 83.170.116.39 [reverse DNS - server42291.uk2net.com]

## 5 Results for 83.170.116.39 (Advancedcleaner.com)

|                             |            |            |            |
|-----------------------------|------------|------------|------------|
| 1. Advancedcleaner.com      | 0 listings | 0 listings | 0 listings |
| 2. Errordigger.com          | 0 listings | 0 listings | 0 listings |
| 3. Pcsupercharger.com       | 0 listings | 0 listings | 0 listings |
| 4. Performanceoptimizer.com | 0 listings | 0 listings | 0 listings |
| 5. Selvascreensaver.com     | 0 listings | 0 listings | 0 listings |



# DomainTools

Reverse-IP

Search Again

IP Address/Hostname: 85.17.4.103

IP Search

Examples: 127.% or 127.0.0.1 - Reverse-IP lookups today: 2/1,000

## Search Results for 85.17.4.103 [no reverse DNS set]

### 13 Results for 85.17.4.103

|                             |            |            |            |
|-----------------------------|------------|------------|------------|
| 1. Antivirussecuritypro.com | 0 listings | 0 listings | 0 listings |
| 2. Errorpatrol.com          | 0 listings | 0 listings | 0 listings |
| 3. Errorprotector.com       | 0 listings | 0 listings | 0 listings |
| 4. Evidenceeraserpro.com    | 0 listings | 0 listings | 0 listings |
| 5. R2d2advertising.com      | 0 listings | 0 listings | 0 listings |
| 6. Supportsw.com            | 0 listings | 0 listings | 0 listings |
| 7. Sysprotect.com           | 0 listings | 0 listings | 0 listings |
| 8. Theringtonsource.com     | 0 listings | 0 listings | 0 listings |
| 9. Virussw.com              | 0 listings | 0 listings | 0 listings |
| 10. Drivecleaner.com        | 0 listings | 0 listings | 0 listings |
| 11. Systemdoctor.com        | 0 listings | 0 listings | 0 listings |
| 12. Winantivirus.com        | 1 listings | 0 listings | 1 listings |
| 13. Winantiviruspro.com     | 0 listings | 0 listings | 0 listings |



## Reverse-IP

Search Again

IP Address/Hostname:  IP Search

Reverse-IP lookups today: 1/1,000

### Search Results for 190.15.73.254 [reverse DNS - 190-15-73-254.securehost.com]

112 Results for 190.15.73.254 (Netmediagroup.net)

|                              |            |            |            |
|------------------------------|------------|------------|------------|
| 1. Ad2cash.net               | 0 listings | 0 listings | 0 listings |
| 2. Ad2profit.com             | 0 listings | 0 listings | 0 listings |
| 3. Adcomatoz.com             | 0 listings | 0 listings | 0 listings |
| 4. Adgurman.com              | 0 listings | 0 listings | 0 listings |
| 5. Adhokuspokus.com          | 0 listings | 0 listings | 0 listings |
| 6. Adnetserver.com           | 0 listings | 0 listings | 0 listings |
| 7. Adredired.com             | 0 listings | 0 listings | 0 listings |
| 8. Adsolutio.com             | 0 listings | 0 listings | 0 listings |
| 9. Adtraff.com               | 0 listings | 0 listings | 0 listings |
| 10. Adverdaemon.com          | 0 listings | 0 listings | 0 listings |
| 11. Adverlounge.com          | 0 listings | 0 listings | 0 listings |
| 12. Adzyclon.com             | 0 listings | 0 listings | 0 listings |
| 13. Antivirussecuritypro.com | 0 listings | 0 listings | 0 listings |
| 14. Astalaprofit.com         | 0 listings | 0 listings | 0 listings |
| 15. B2adz.com                | 0 listings | 0 listings | 0 listings |
| 16. Bestadmedia.com          | 0 listings | 0 listings | 0 listings |
| 17. Bestpharmacydeals.com    | 0 listings | 0 listings | 0 listings |
| 18. Bestsearchnet.com        | 0 listings | 0 listings | 0 listings |
| 19. Bestshopz.com            | 0 listings | 0 listings | 0 listings |
| 20. Bestwnvmovies.com        | 0 listings | 0 listings | 0 listings |
| 21. Bizadverts.com           | 0 listings | 0 listings | 0 listings |
| 22. Bizmarketads.com         | 0 listings | 0 listings | 0 listings |
| 23. Blessedads.com           | 0 listings | 0 listings | 0 listings |
| 24. Brandmarketads.com       | 0 listings | 0 listings | 0 listings |
| 25. Bucksinsoft.com          | 0 listings | 0 listings | 0 listings |
| 26. Burnads.com              | 0 listings | 0 listings | 0 listings |
| 27. Cancerno.com             | 0 listings | 0 listings | 0 listings |
| 28. Cashloanprofit.com       | 0 listings | 0 listings | 0 listings |
| 29. Casinoaceking.com        | 0 listings | 0 listings | 0 listings |

|                              |            |            |            |
|------------------------------|------------|------------|------------|
| 30. Casinodealsgalore.com    | 0 listings | 0 listings | 0 listings |
| 31. Cheap-auto-deals.com     | 0 listings | 0 listings | 0 listings |
| 32. Co-search.com            | 0 listings | 0 listings | 0 listings |
| 33. Deuscleanerpay.com       | 0 listings | 0 listings | 0 listings |
| 34. Easybestdeals.com        | 0 listings | 0 listings | 0 listings |
| 35. Eroticabsolute.com       | 0 listings | 0 listings | 0 listings |
| 36. Fantazybill.com          | 0 listings | 0 listings | 0 listings |
| 37. Favouriteshop.com        | 0 listings | 0 listings | 0 listings |
| 38. Fileprotector.com        | 0 listings | 0 listings | 0 listings |
| 39. Forceup.com              | 0 listings | 0 listings | 0 listings |
| 40. Freepcsecure.com         | 0 listings | 0 listings | 0 listings |
| 41. Freetvnow.net            | 0 listings | 0 listings | 0 listings |
| 42. Friedads.com             | 0 listings | 0 listings | 0 listings |
| 43. Getfreecar.com           | 0 listings | 0 listings | 0 listings |
| 44. Glorymarkets.com         | 0 listings | 0 listings | 0 listings |
| 45. Great4mac.com            | 0 listings | 0 listings | 0 listings |
| 46. Greyhathosting.com       | 0 listings | 0 listings | 0 listings |
| 47. Hebooks-service.com      | 0 listings | 0 listings | 0 listings |
| 48. Iddqdmartketing.com      | 0 listings | 0 listings | 0 listings |
| 49. Infyte.com               | 0 listings | 0 listings | 0 listings |
| 50. Installprovider.com      | 0 listings | 0 listings | 0 listings |
| 51. Internetadaultfriend.com | 0 listings | 0 listings | 0 listings |
| 52. Intervarioclick.com      | 0 listings | 0 listings | 0 listings |
| 53. Invulnerableads.com      | 0 listings | 0 listings | 0 listings |
| 54. Keywordcpv.com           | 0 listings | 0 listings | 0 listings |
| 55. Libresystm.com           | 0 listings | 0 listings | 0 listings |
| 56. Luckyadcoin.com          | 0 listings | 0 listings | 0 listings |
| 57. Luckyadsols.com          | 0 listings | 0 listings | 0 listings |
| 58. Magicsearcher.com        | 0 listings | 0 listings | 0 listings |
| 59. Manage-search.com        | 0 listings | 0 listings | 0 listings |
| 60. Marketingdungeon.com     | 0 listings | 0 listings | 0 listings |
| 61. Mediatornado.com         | 0 listings | 0 listings | 0 listings |
| 62. Megashopcity.com         | 0 listings | 0 listings | 0 listings |
| 63. Mightyfaq.com            | 0 listings | 0 listings | 0 listings |
| 64. Misc-search.com          | 0 listings | 0 listings | 0 listings |
| 65. Mobilesoftmarketing.com  | 0 listings | 0 listings | 0 listings |
| 66. Moneycometrue.com        | 0 listings | 0 listings | 0 listings |
| 67. Moneypalacecash.com      | 0 listings | 0 listings | 0 listings |
| 68. Myfavouritesearch.com    | 0 listings | 0 listings | 0 listings |
| 69. Myhealth-life.org        | 0 listings | 0 listings | 0 listings |
| 70. Myonlinefinance.com      | 0 listings | 0 listings | 0 listings |
| 71. Mysurvey4u.com           | 0 listings | 0 listings | 0 listings |
| 72. Mythmarketing.com        | 0 listings | 0 listings | 0 listings |
| 73. Mytravelgeek.com         | 0 listings | 0 listings | 0 listings |
| 74. Netmediagroup.net        | 0 listings | 0 listings | 0 listings |

|                            |            |            |            |
|----------------------------|------------|------------|------------|
| 75. Netturbopro.com        | 0 listings | 0 listings | 0 listings |
| 76. Onestopshopz.com       | 0 listings | 0 listings | 0 listings |
| 77. Opensols.com           | 0 listings | 0 listings | 0 listings |
| 78. Pcsoftw.com            | 0 listings | 0 listings | 0 listings |
| 79. Pcsupercharger.com     | 0 listings | 0 listings | 0 listings |
| 80. Popadprovider.com      | 0 listings | 0 listings | 0 listings |
| 81. Popsmedia.com          | 0 listings | 0 listings | 0 listings |
| 82. Popupnukerpro.com      | 0 listings | 0 listings | 0 listings |
| 83. Prenetsearch.com       | 0 listings | 0 listings | 0 listings |
| 84. Prevedmarketing.com    | 0 listings | 0 listings | 0 listings |
| 85. Prizesforyou.com       | 0 listings | 0 listings | 0 listings |
| 86. R2d2advertising.com    | 0 listings | 0 listings | 0 listings |
| 87. Rocktheads.com         | 0 listings | 0 listings | 0 listings |
| 88. Roller-search.com      | 0 listings | 0 listings | 0 listings |
| 89. Rombic-search.com      | 0 listings | 0 listings | 0 listings |
| 90. Searchcolours.com      | 0 listings | 0 listings | 0 listings |
| 91. Sellmoresoft.com       | 0 listings | 0 listings | 0 listings |
| 92. Selvascreensaver.com   | 0 listings | 0 listings | 0 listings |
| 93. Sharpadverts.com       | 0 listings | 0 listings | 0 listings |
| 94. Shivanetworking.com    | 0 listings | 0 listings | 0 listings |
| 95. Shopshot.com           | 0 listings | 0 listings | 0 listings |
| 96. Softwcs.com            | 0 listings | 0 listings | 0 listings |
| 97. Stratosearch.com       | 0 listings | 0 listings | 0 listings |
| 98. Swiftcleaner.com       | 0 listings | 0 listings | 0 listings |
| 99. Tallgrass-seach.com    | 0 listings | 0 listings | 0 listings |
| 100. Traffalo.com          | 0 listings | 0 listings | 0 listings |
| 101. Traveltray.com        | 0 listings | 0 listings | 0 listings |
| 102. Uniqads.com           | 0 listings | 0 listings | 0 listings |
| 103. Vitecmmedia.com       | 0 listings | 0 listings | 0 listings |
| 104. Waytotheprofit.com    | 0 listings | 0 listings | 0 listings |
| 105. Windefender.com       | 0 listings | 0 listings | 0 listings |
| 106. Wontu-search.com      | 0 listings | 0 listings | 0 listings |
| 107. Workhomecenter.com    | 0 listings | 0 listings | 0 listings |
| 108. Yourseeker.com        | 0 listings | 0 listings | 0 listings |
| 109. Yourshopz.com         | 0 listings | 0 listings | 0 listings |
| 110. Yourteacheronline.com | 0 listings | 0 listings | 0 listings |
| 111. Zappinads.com         | 0 listings | 0 listings | 0 listings |
| 112. Zooworld-search.com   | 0 listings | 0 listings | 0 listings |

Attachment H

Page 282



Print Window | Close Window

Search Terms: Company Name: Winsoftware

Document 3 of 4  
Copyright 2008 Dun & Bradstreet, Inc  
Worldbase  
RETURN

Check availability of a D&amp;B Business Information Report (Credit Report)

December 3, 2005

**WINSOFTWARE LTD**

GREEN DRAGON HOUSE  
64-70 HIGH STREET  
CROYDON CR0 1NA  
ENGLAND

**REGION:** EUROPE\*\*\*\*\* **COMPANY IDENTIFIERS** \*\*\*\*\***DUNS:** 73-522-9499**NATIONAL:** 4785713-UK Cro Number**CLASS CODE:** 7372 -1972 SIC CODE\*\*\*\*\* **COMPANY INFORMATION** \*\*\*\*\***LEGAL STATUS:** Corporation**COMPANY TYPE:** Private\*\*\*\*\* **EXECUTIVES** \*\*\*\*\***CEO:** DANIEL SUNDIN, DIRECTOR\*\*\*\*\* **DESCRIPTION** \*\*\*\*\*

PREPACKAGED SOFTWARE

\*\*\*\*\* **MARKET AND INDUSTRY** \*\*\*\*\***SIC CODES:**

7372 - Prepackaged software services

\*\*\*\*\* **FINANCIALS** \*\*\*\*\***FISCAL YEAR DATE:** June 30, 2004\*\*\*\*\* **OTHER FINANCIALS** \*\*\*\*\***FINANCIAL FIGURE DATE** 06/30/2004**US DOLLARS****UK Pound Sterling**

NET WORTH

**LOAD-DATE:** April 10, 2008

WinSoftware - Windows Internet Explorer  
http://www.winsoftware.com/store/

WinSoftware  
Professional security for home computing

Store

Cart Login

Search the Store

**WinSoftware**

**STORE**

- Virus Protection
- Content Filtering
- Privacy Protection
- Advertising Filtering
- System Optimization

• About WinSoftware

• Privacy Policy

• Cancellation

• Refund and Return Policy

**WinPrivacyGuard**  
Just  
**39<sup>95</sup>**  
WinPrivacyGuard 2005 is a comprehensive utility which monitors and safeguards private information stored on your system from being revealed to unauthorized sources  
[more info](#)  
[Buy Now](#)

**WinAntiVirus 2005 Pro**  
Just  
**49<sup>95</sup>**  
This one-of-its-kind software has the antivirus, firewall, anti-spy and the popup utilities all packed into one.  
[more info](#)  
[Buy Now](#)

**WinAntiSpam 2005**  
Just  
**39<sup>95</sup>**  
WinAntiSpam 2005's is a utility that effectively filters all junk mails. This easy-to-use program connects with the worldwide spam database and sends automated replies to users to conf  
[more info](#)  
[Buy Now](#)

**WinContentFilter**  
Just  
**29<sup>95</sup>**  
Protect your family from non advisable contents. Filters out offensive text on web sites, emails and other text files. Scans hard drive for unscrupulous contents  
[more info](#)  
[Buy Now](#)

Don't WinSoftware Privacy Policy Cancellation Refund and Return Policy

Copyright © 2005 WinSoftware. All Rights Reserved.  
All materials on this site are property of WinSoftware.

About WinSoftware - Windows Internet Explorer  
http://www.winsoftware.com/store/about.html

About WinSoftware

WinSoftware™  
Professional security for home computing

Store

Cart Login

Search the Store

### WinSoftware – About Us

WinSoftware is a world-class business services company focused on delivering first-class security solutions to a wide range of clients. Their software secures, protects, and optimizes the computers of consumers and home office users.

Win's advanced retail desktop solutions include leading anti-virus, security, encryption, and desktop optimization software. Win's managed Web security services employ a patented system and process of delivering software through an Internet browser to provide these services to users online through our web site.

- ▶ Virus Protection
- ▶ Content Filtering
- ▶ Privacy Protection
- ▶ Advertising Filtering
- ▶ System Optimization

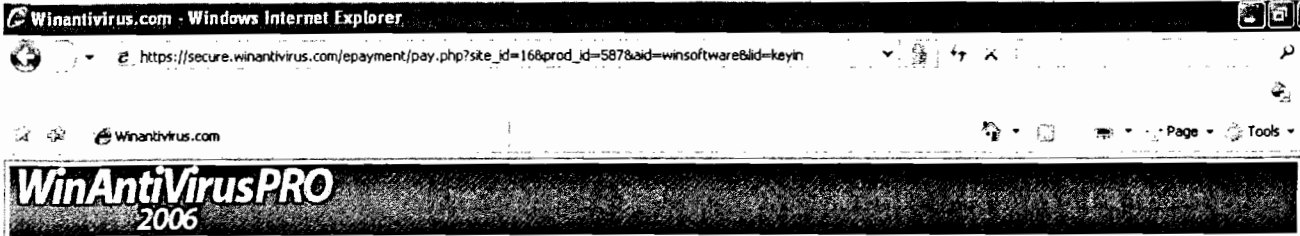
About Us


- ▶ About WinSoftware
- ▶ Privacy Policy
- ▶ Cancellation
- ▶ Refund and Return Policy

WinSoftware | Privacy Policy | About Us | Refund and Return Policy

Copyright © 2005 WinSoftware. All Rights Reserved.  
All materials on this site are property of WinSoftware.

1:03:22 PM 5/2/2008



|  | Description                                                                                                                                                        | Price         |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
|                                                                                   | Complete Security Suite - Professional Pack                                                                                                                        |               |
|                                                                                   | <b>WinAntivirus Pro 2006</b> - Includes <b>ANTI-SPYWARE, ANTI-VIRUS, FIREWALL &amp; POPUP BLOCKER!</b><br>PRO 4-in-1 Suite - <b>Save Over 70% on a \$149 Value</b> |               |
|                                                                                   | <input type="radio"/> One Year Unlimited Protection                                                                                                                | \$49.95       |
|                                                                                   | <input checked="" type="radio"/> Monthly Subscription - You will automatically be re-billed monthly.                                                               | \$2.95 /month |

**Billing Information:**

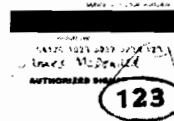
\* Card Number

(Numbers only no spaces or dashes)

Expiry Date  
(MM/YYYY)

05 2008

Card ID Number



The CVV2 code is the three-digit code located after the credit card number on the signature strip of Visa and Master Card cards (see example above)

\* First Name

\* Last Name

Phone

\* Address

\* City

\* Country

State / Province (For US/Canada Only)

\* Zip Code

 United States  
 Select From List

Type your email address and select a password. You'll use these each time you access the Members Area. Please note that both your username and password are case sensitive

\* Email Address

\* Re-Enter Email Address

\* Password

Password must be between 4 and 25 characters

☒ I agree to the [Terms and Conditions](#) & [License Agreement](#)

Secure Purchase

Please click only once!



Store

Cart Login

## Search the Store

- » Virus Protection
- » Content Filtering
- » Privacy Protection
- » Advertising Filtering
- » System Optimization

## About Us

- » About WinSoftware
- » Privacy Policy
- » Cancellation

## » Refund and Return Policy

## WinSoftware — Refund and Return Policy

Refund issue will not be considered if a Supporter Tool log has not been submitted.

This will let the Technical Department analyze all possible issues, find reasons and provide solutions for them.

Our 24/7 customer support service should be contacted for any troubleshooting. Customer support service should be informed in the event the customer's system crashed for any reason, in order for the customer to be entitled to claim a refund. If the support team is not contacted, a refund will NOT be made.

This reduces all problems to technical difficulties which will be researched and solved.

Win Software? Ltd. is not responsible for any help the customer gets from third party technicians. Also any actions taken by the customer are made at his or her risk.

Some of our products may be unsuited to run with other software. We have the right to uninstall incompatible products. We will notify our customers before uninstalling such products. A customer CANNOT claim a refund if the reason is a requisition or removal of conflicting software.

Cocexistence of some products may lead to many unsatisfactory effects as well as to slow the customer's system. That is why the usage of [Product Name] requires the uninstallation of products which represent a risk to the system.

Customers CANNOT demand a refund on Software if the problem is not related to that particular software. We declare the functionality of all Software we sell. Refunds will not be granted on the grounds of the Software not performing any function it was not originally intended to perform. The issues the customer faces can be related to the interaction of the Software with different systems or other software. Win Software? Ltd. is not responsible for any harmful interactions.

In this case the Technical department will analyze the customer's system data and reports possible reasons for the problem.

We are not liable if the customer's system was restored or repaired and a refund will NOT be made in such a case.

In a few cases, protection-related [Product Name] cannot deal with overloaded and damaged systems. In such cases, the Win Software? Ltd. is not responsible.

Win Software? Ltd. cannot be held responsible for actions performed by the customer when not using our Software.

If the customer has problems downloading [Product Name] he or she may contact the customer support service which will provide them with an alternative method within 72 hours after the complaint was filed. Declaring a refund is NOT possible without installing and a 7-days trial procedure.

Partial refunds for defective [Product Name] may be granted if the product has been acquired as part of a bundled purchase.

Refunds will not be given because of wrong or improper software settings set. Instructions on correct settings are described in the manual and can be also requested through the software's web site or Customer Support Service.

Refunds will not be given for not providing software burned on CD or any other media. There is no charge for CD cost or shipping. The customer can record software downloaded from Internet to CD or any other media for non-commercial purposes.

Monthly subscription customers may only claim for refund for following months or within the first five days of the current month. Refunds will not be given for previous months.

top



We accept Visa, Master Card, American Express, Discover.

WinAntivirus Pro 2006 LICENSE AGREEMENT:

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING WinAntivirus Pro 2006. WINSOFTWARE Corporation, Inc. AND/OR ITS SUBSIDIARIES ARE WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING WinAntivirus Pro 2006 (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND WINSOFTWARE Corporation, Inc. BY CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL; MAKE NO FURTHER USE OF THE SOFTWARE, AND CONTACT THE CUSTOMER SUPPORT TEAM.

1. License.

The software which accompanies this license (collectively the "Software") is the property of WINSOFTWARE Corporation, Inc. or its licensors and is protected by copyright law. While WINSOFTWARE Corporation, Inc. continues to own WinAntivirus Pro 2006, You will have certain rights to use WinAntivirus Pro 2006 after Your acceptance of this license. This license governs any releases, revisions, or enhancements to WinAntivirus Pro 2006 that WINSOFTWARE Corporation, Inc. may furnish to You.

Your rights and obligations with respect to the use of this Software are as follows:

You may:

- A. use one copy of WinAntivirus Pro 2006 on one (1) single computer during subscription period;
- B. make one copy of WinAntivirus Pro 2006 for archival purposes, or copy the WinAntivirus Pro 2006 onto the hard disk of Your computer and retain the original for archival purposes;
- C. use WinAntivirus Pro 2006 on a network, provided that You have a licensed copy of WinAntivirus Pro 2006 for each computer that can access WinAntivirus Pro 2006 over that network; and
- D. after written permission from WINSOFTWARE Corporation, Inc., transfer WinAntivirus Pro 2006 on a permanent basis to another person or entity, provided that You retain no copies of WinAntivirus Pro 2006 and the transferee agrees to the terms of this license;
- E. be informed of any changes or updates regarding the WinAntivirus Pro 2006 by e-mail or any other contact method available.

You may not:

- A. copy the printed documentation which may accompany WinAntivirus Pro 2006;
- B. sublicense, rent or lease any portion of WinAntivirus Pro 2006; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of WinAntivirus Pro 2006, or create derivative works from WinAntivirus Pro 2006;
- C. use a previous version or copy of WinAntivirus Pro 2006 after You have received a disk replacement set or an upgraded version. Upon upgrading the Software all copies of the prior

**Bank of America Secured Card Application**

Please bring this application with you when you open your Bank of America savings account.

Important: To ensure prompt processing, please print and fill out completely. Note: If married, you may apply for a separate account in your own name.

Type of Account ☐ Visa\* ☒ Gold (\$250 - \$4999) or ☐ Platinum (\$5000 - \$10,000)**BANKING RELATIONSHIP**Do you have a banking relationship with Bank of America? ☒ YES ☐ NO

If yes, please list your account number below:

Checking Account #: [REDACTED]

Savings Account #: [REDACTED]

OVERDRAFT PROTECTION: Please indicate how you desire Automatic Overdraft Protection.

**1 Please tell us about yourself**

|                                                                                                                |                 |                            |
|----------------------------------------------------------------------------------------------------------------|-----------------|----------------------------|
| First Name<br><b>DANIEL SUNDIN</b>                                                                             | MI<br><b>MI</b> | Last Name<br><b>SUNDIN</b> |
| Social Security Number<br>[REDACTED]                                                                           |                 |                            |
| Area Code & Phone Number<br><b>(623) 322-5210</b>                                                              |                 |                            |
| Date of Birth (MM/DD/YY)<br><b>11/23</b>                                                                       |                 |                            |
| Home Address or Post Office Box<br><b>17600 N 19th AVE</b>                                                     |                 |                            |
| City<br><b>GLENDALE</b>                                                                                        |                 |                            |
| State<br><b>AZ</b>                                                                                             |                 |                            |
| Zip<br><b>85306</b>                                                                                            |                 |                            |
| Email Address (Work/Home)<br><b>daniel.sundin@csdhs.org</b>                                                    |                 |                            |
| Are you a U.S. citizen or a permanent resident of the U.S.? <input type="radio"/> Yes <input type="radio"/> No |                 |                            |
| Are you a non-resident alien? <input type="radio"/> Yes <input type="radio"/> No                               |                 |                            |
| Monthly Payment<br><b>\$ 910</b>                                                                               |                 |                            |
| <input type="radio"/> Rent <input type="radio"/> Mortgage                                                      |                 |                            |
| Bank of America Customer Since (MM/YY)<br><b>01/01</b>                                                         |                 |                            |

**2 Please tell us about your employment or source(s) of income**

|                                                                       |                                                                           |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------|
| Name of Current Employer or Business<br><b>VANTAGE SOFTWARE, INC.</b> | Annual Gross Household Income<br><b>\$ 120,000.00</b>                     |
| Area Code & Work Phone<br><b>(602) 925-7410</b>                       | <input type="radio"/> Indirect <input type="radio"/> Permanently Disabled |

**3 Co-applicant's information**

|                                         |                  |                         |
|-----------------------------------------|------------------|-------------------------|
| Co-Applicant's First Name<br>[REDACTED] | MI<br>[REDACTED] | Last Name<br>[REDACTED] |
| Social Security Number<br>[REDACTED]    |                  |                         |

**4 Yes, I want a free additional card**

|                                      |                  |
|--------------------------------------|------------------|
| First Name<br>[REDACTED]             | MI<br>[REDACTED] |
| Last Name<br>[REDACTED]              |                  |
| Social Security Number<br>[REDACTED] |                  |

**5 Optional Payment Protection Plan**

You may enroll in the optional Payment Protection Plan offered through Bank of America Business Services, Inc. and administered by Citicard Bank of America. I authorize Bank of America to provide my name, address, phone number and date of birth to Citicard Bank in order to receive my coverage. I understand that I have received the following disclosure which is posted in the form. This business product is not insured by the FDIC, any other agency of the United States, or by the bank. It is not a deposit or other obligation of the bank. It is not guaranteed or underwritten by the bank. It is not a substitute for any bank service. You are not required to purchase insurance from the bank or its affiliate, nor are you prohibited from purchasing insurance from an unaffiliated entity in order to receive an exception of credit from the bank. This product is not available in AL, HI, IL & NY.

Form B0901TK0

YES

Sign Here to Enroll

NO

Sign Here to Decline

**6 Signatures for agreement**

Note: Application cannot be processed without signature(s).

By signing below, you agree to the authorizations, terms and conditions on the reverse side.

|                          |                         |
|--------------------------|-------------------------|
| <b>x Daniel Sundin</b>   | Date<br><b>12/27/08</b> |
| Your Signature           | Date                    |
| <b>x [REDACTED]</b>      | Date                    |
| Co-Applicant's Signature | Date                    |

**Bank of America Representative:**

Please fill in the following and forward Application to AZB-904-02-01:  
Our customer can deposit any amount between \$250 and \$10,000 in \$50 increments.  
Deposit Amount \$ **322.00** (Credit Limit Requested - minimum \$250)

FUNDING OF SECURITY DEPOSIT: (check only one box)  
☐ Cashier's Check ☐ Money Order ☐ Personal Check ☒ Cash  
Banking Center # **8374** **12/27/08** Signature Initials **DS**  
Bank of America Customer Since (MM/YY) **12/27/01**

App Type: SCM Tracking ID# 4340

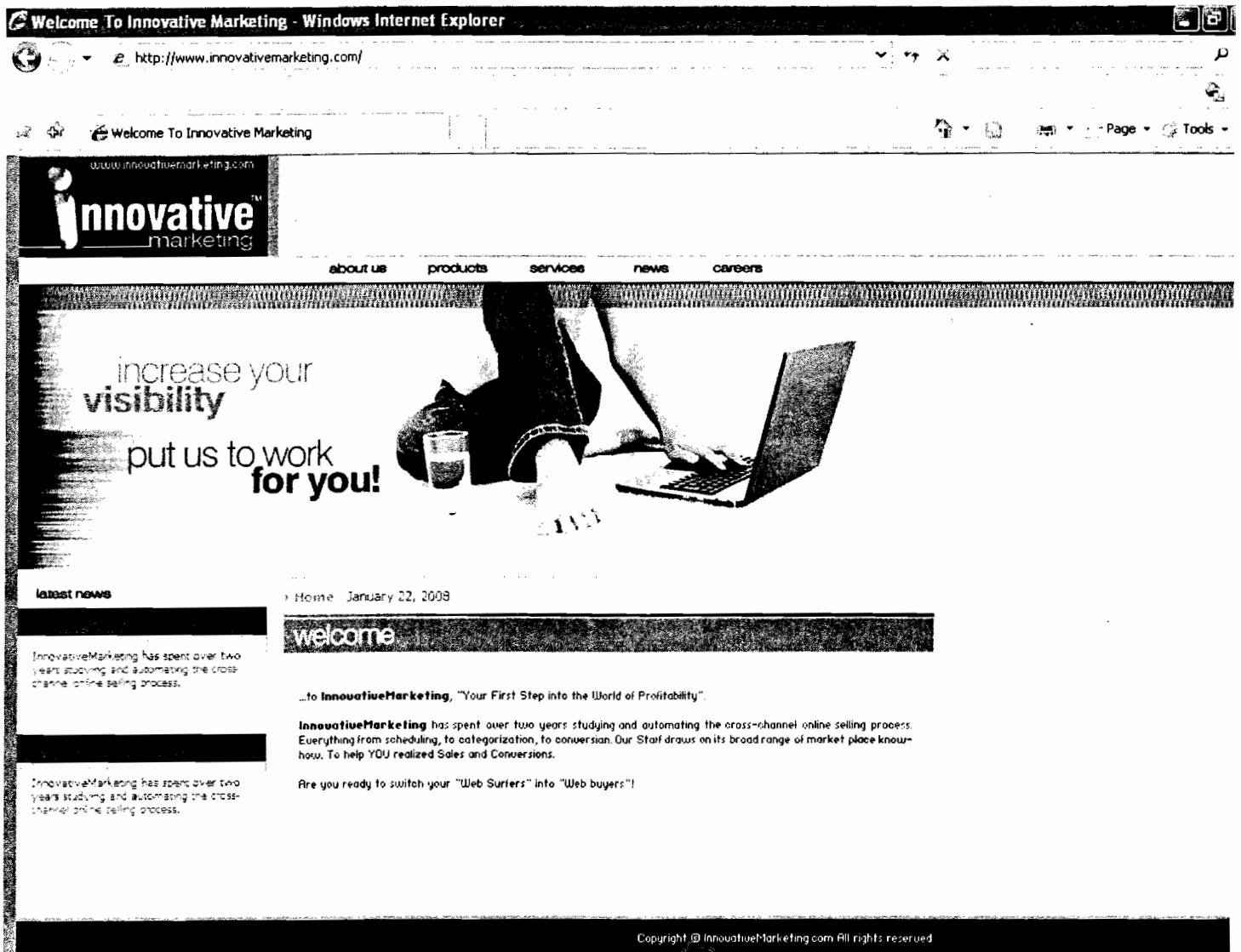
95-02-20288 (09/2001)

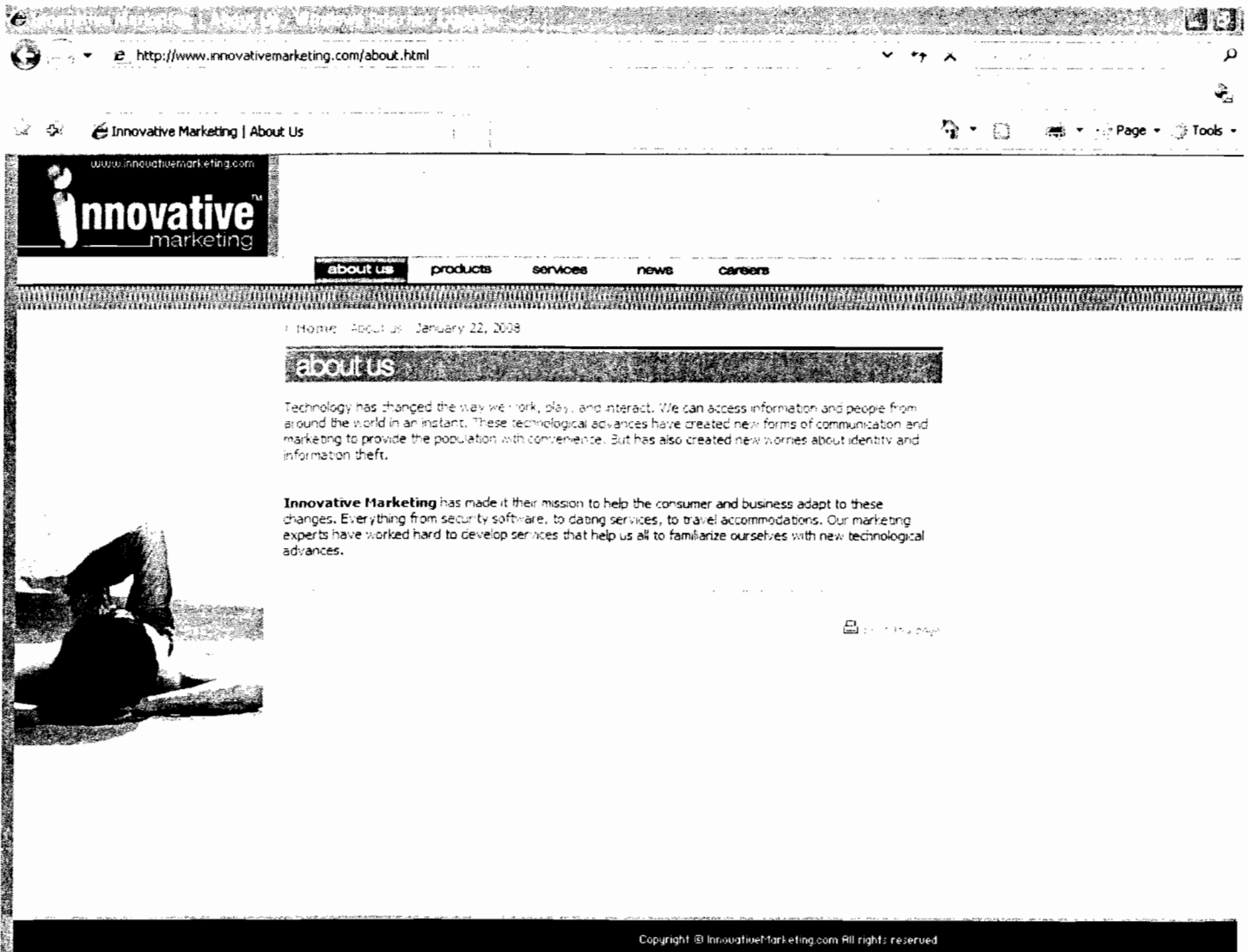
OCR# 25001

Place Banking Center ID Stamp Here

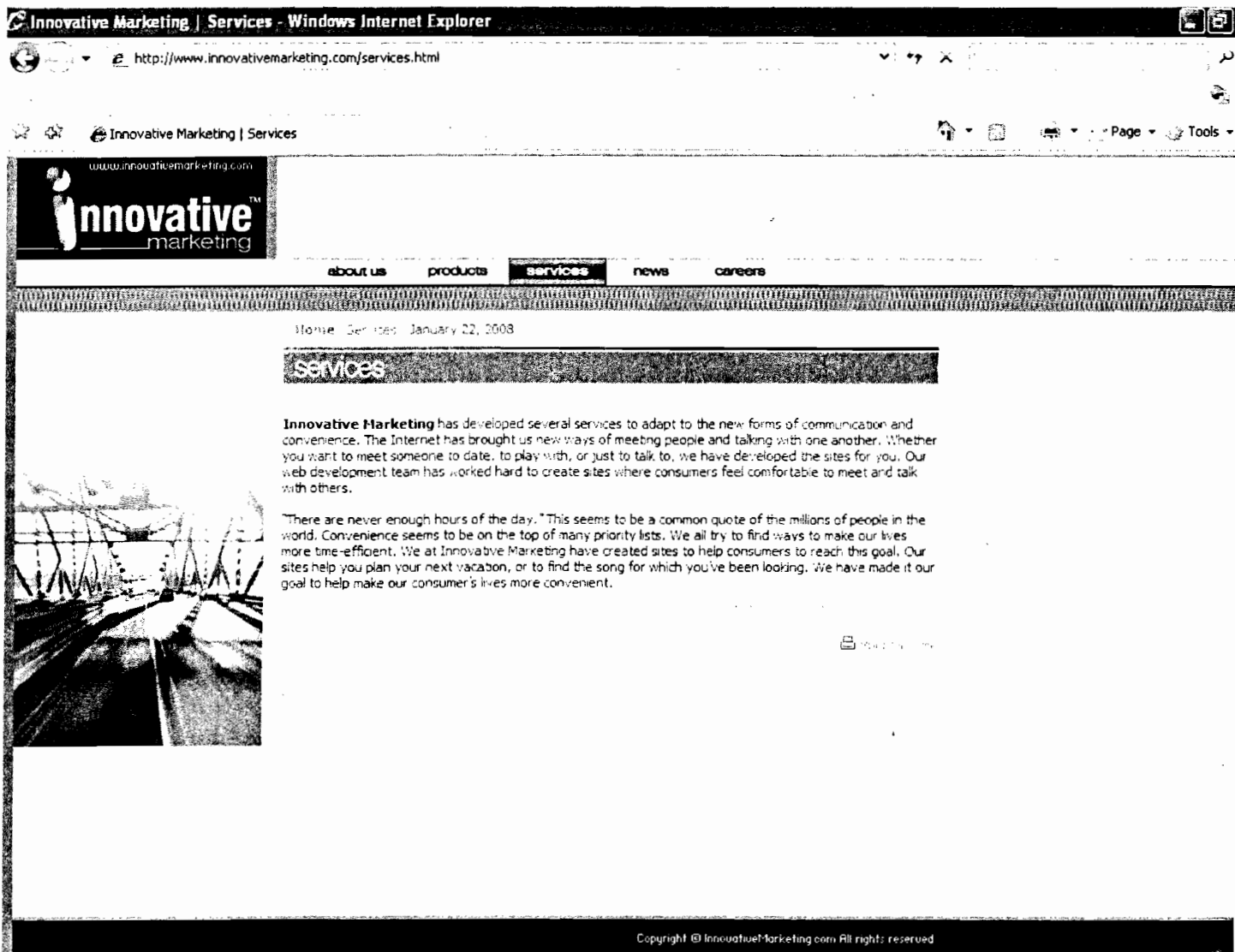
**AZ1- [REDACTED] 630259**  
**333 0002761**

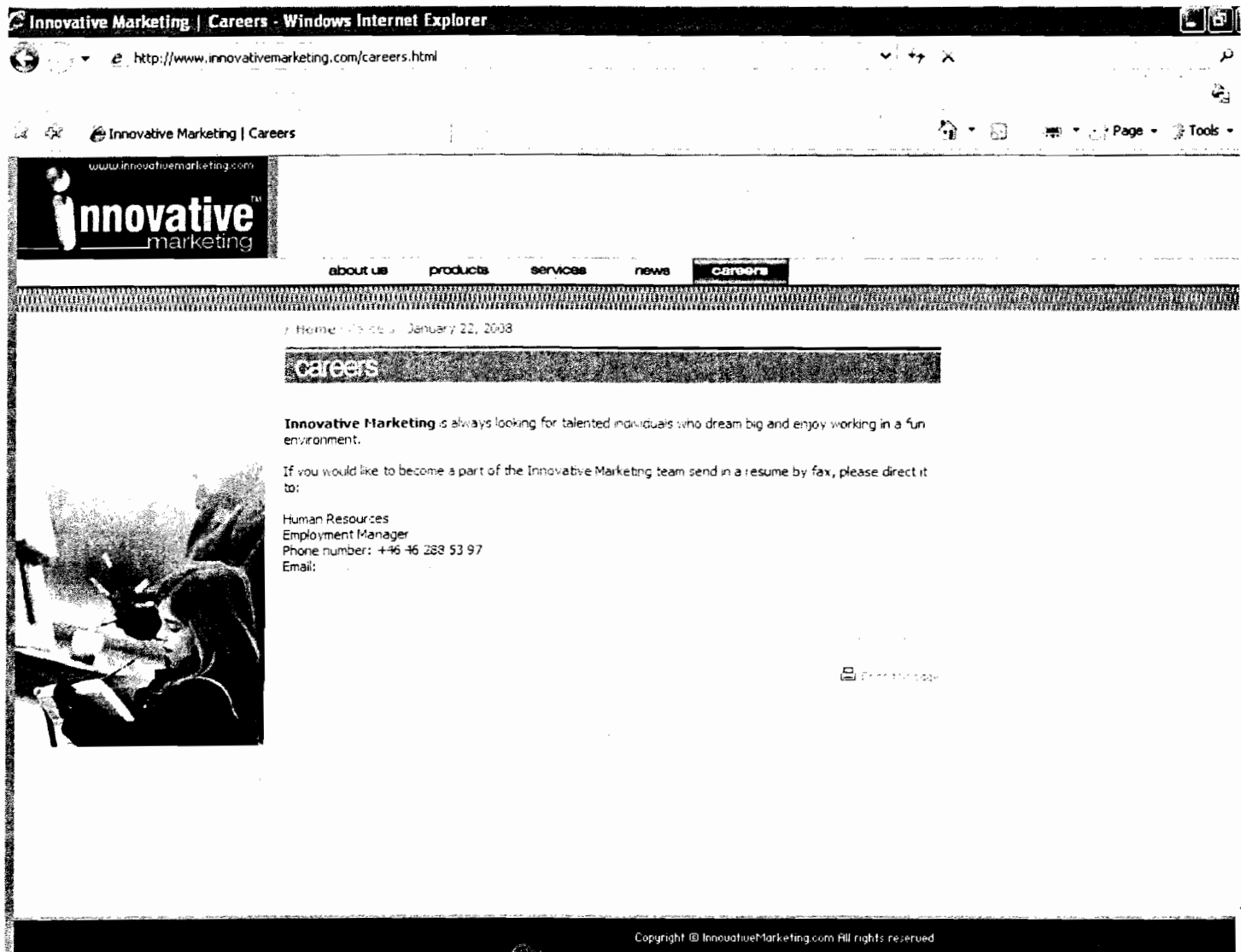
1:11:12 PM 5/2/2008













Windows Live™ Hotmail


## Your WinAntiSpyware 2007 order

From: **support@winantispyware.com**

Sent: Thu 8/02/07 2:11 PM

To: jcbUTTONS@hotmail.com

Attachments: dots.gif (0.1 KB), was7.gif (3.2 KB)

Security scan upon download 



To: Jamie Cooper

From: WinAntiSpyware Support Department

Subject: Your WinAntiSpyware 2007 order

If you have faced any issues to download or install WinAntiSpyware 2007 software please kindly use direct link: WinAntiSpyware 2007

**Dear Jamie Cooper,**

Thank you for your order.

**Product:** WinAntiSpyware 2007

**Site:** winantispyware.com

**Order Billed As:** virussw.com 8007555909

**Order Number:** 4812547

Your Software can be downloaded from this link

**User name:** jcbUTTONS@hotmail.com

**Password:** WJ50LGsR

**BILLING INFORMATION:** Your Charge Description will appear as "**virussw.com 8007555909**" for the purchase of WinAntiSpyware 2007 from **winantispyware.com** for **39.95 USD**.

For your convenience, we have created a very user-friendly and informative FAQ section, which lists answers to many commonly asked questions. Please refer to this section for answers to your questions. And also a guide link for InstallationGuide  
Extended Download Service

a. Your order is a downloadable product under Extended Download Service from our stores, you are automatically granted a 12 month access in which your purchase can be re-downloaded at any time.

b. Shipping of a Product CD is not available with this offer

Please be informed that from now on you have a full access to our Member's Area where you can clarify all the doubts you have regarding usage of your software.

Please allow our support division a reasonable response time. Also, be sure to include your Order Number in the Subject Line with any correspondence.

Warm Regards,

**WinAntiSpyware 2007 Support Department**

[winantispware.com](http://winantispware.com)

[support@winantispware.com](mailto:support@winantispware.com)

**+1. (202) 904-2212 (24/7 Phone Support)**

**+1. (800) 755-5909 (24/7 Toll-Free USA Phone Support)**

**+1. (800) 889-5113 (24/7 Toll-Free Canada Phone Support)**

**+61 (290) 372-132 (24/7 Phone Support Australia)**

**+44 (120) 925-01-11 (24/7 Phone Support UK)**

This e-mail is confidential and non-SPAM. If you received this message by mistake, please delete all copies from your system and notify the sender immediately by return e-mail. The sender does not accept liability for any errors or omissions.

Letter content was scanned

No threat detected

**winantispware.com**

|  |            |        |        |  |
|--|------------|--------|--------|--|
|  | 09/09/2007 | \$0.00 | \$0.00 |  |
|--|------------|--------|--------|--|

|||||.....  
JAMIE COOPER  
N00003

CITIBANK  
P.O. BOX 6575  
THE LAKES, NEVADA  
88901-6575

For a credit balance refund, or a telephone or address change, please place an X in the parentheses and make the desired changes on the reverse side. Thank you.

Payment coupon: Please tear along perforation and return this portion with your payment. Make check or money order payable in U.S. dollars on a U.S. bank to Citibank. Include account number on check or money order. No cash please. Do not staple or tape your check to this coupon.

## CITIBANK CORPORATE CARD

Statement Date  
08/15/07

Payment Date  
09/09/07

| Previous Balance | Payments | Credits | Purchases and Advances | Interest Charges |
|------------------|----------|---------|------------------------|------------------|
| \$0.00           | \$0.00   | \$0.00  | \$0.00                 | \$3,000          |

For customer service call or write 1-800-248-4553 P.O. Box 6125 Sioux Falls, SD 57117

Send payments to: Citibank P.O. Box 6575 The Lakes, Nevada 88901-6575

| Account Number                                                                                                                                                                                                                                                                                                                                                                               |           | Cash Advance Limit | Available Credit Line | Available Cash Line** |                        |                               |             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------------------|-----------------------|-----------------------|------------------------|-------------------------------|-------------|
|                                                                                                                                                                                                                                                                                                                                                                                              |           | \$3,000            | \$3,000               | \$3,000               |                        |                               |             |
| Sale Date                                                                                                                                                                                                                                                                                                                                                                                    | Post Date | Reference Number   | Type of Activity      | Amount                |                        |                               |             |
| <p>-----NOTICE MEMO ITEMS LISTED BELOW-----</p> <p>08/02 08/03 74547717214201388466181 SUPPORTSW.COM 8007555908 PALMA MALLORC 39.95</p> <p>----- TOTAL AMOUNT OF MEMO ITEM(S): 70.90 -----</p>                                                                                                                                                                                               |           |                    |                       |                       |                        |                               |             |
| <p>Your international transactions include a service fee of 1% assessed to Citibank by the applicable bankcard association. For international transactions converted from a foreign currency to U.S. dollars by us, the service fee is included in the currency conversion rate. For all other international transactions, the service fee is included in the posted transaction amount.</p> |           |                    |                       |                       |                        |                               |             |
| ACCOUNT SUMMARY                                                                                                                                                                                                                                                                                                                                                                              |           | Previous Balance   | Payments              | Credits               | Purchases and Advances | Interest Charges              | New Balance |
| CURRENT PERIOD                                                                                                                                                                                                                                                                                                                                                                               |           |                    |                       |                       |                        |                               |             |
| Purchases                                                                                                                                                                                                                                                                                                                                                                                    |           | 0.00               |                       |                       |                        |                               | 0.00        |
| Advances                                                                                                                                                                                                                                                                                                                                                                                     |           | 0.00               |                       |                       |                        |                               | 0.00        |
| TOTALS                                                                                                                                                                                                                                                                                                                                                                                       |           | 0.00               |                       |                       |                        |                               | 0.00        |
| DAYS IN BILLING PERIOD: 31                                                                                                                                                                                                                                                                                                                                                                   |           | Purchases          |                       | Cash Advances         |                        | Payment Due:                  |             |
| Balance Subject To Interest Charges >                                                                                                                                                                                                                                                                                                                                                        |           | .00                |                       | .00                   |                        | Amount Over Credit Limit: .00 |             |
| Periodic Rate >                                                                                                                                                                                                                                                                                                                                                                              |           | .0000%             |                       | .0000                 |                        | Amount Past Due: .00          |             |
| ANNUAL PERCENTAGE RATE >                                                                                                                                                                                                                                                                                                                                                                     |           | .0000%             |                       | .0000                 |                        | MINIMUM AMOUNT DUE: .00       |             |

Order placed: 2008-03-12  
advancedcleaner.com

ORDER #: 6153843

|                                                                                                             |                                                                                                    |                           |
|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|---------------------------|
| <b>Shipping Address:</b><br>Jessie Logan<br>[REDACTED]<br>United States<br><br><b>Shipping:</b><br>Standard | <b>Items Ordered</b><br>1. AdvancedCleaner + Premium Support<br><br>- 1 item(s) Gift options: None | <b>Price</b><br>64.90 USD |
|                                                                                                             | <b>Item(s) Subtotal</b>                                                                            | 64.90 USD                 |
|                                                                                                             | <b>Shipping &amp; Handling:</b>                                                                    | USD 0.00                  |
|                                                                                                             | <b>Subtotal</b>                                                                                    | 64.90 USD                 |
| <b>Total for this Shipment</b>                                                                              |                                                                                                    | 64.90 USD                 |

Your charge will appear as: **supportsw.com 8007555909**

PAYMENT INFORMATION

|                                                                                                                                                                                                   |                                 |           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-----------|
| <b>Payment Method:</b><br>visa<br>Authorization code: 18468530<br>Last 4 digits: 0005<br>Transaction Type: Purchase<br><br><b>Billing Address:</b><br>Jessie Logan<br>[REDACTED]<br>United States | <b>Item(s) Subtotal</b>         | 64.90     |
|                                                                                                                                                                                                   | <b>Shipping &amp; Handling:</b> | USD 0.00  |
|                                                                                                                                                                                                   | <b>Total Before Tax</b>         | 64.90     |
|                                                                                                                                                                                                   | <b>Estimated Tax</b>            | 0         |
|                                                                                                                                                                                                   | <b>Grand Total</b>              | 64.90 USD |

In case of any problems with AdvancedCleaner + Premium Support customer should contact the Customer Support service.

Declaring a refund is NOT possible without contacting our Customer Support Department.

See our Refund Policy.

**Questions?**

**e-mail:** support@advancedcleaner.com

**CUSTOMER SUPPORT**

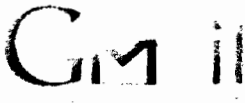
- +1. (202) 904-2212 (24/7 Phone Support)
- +1. (800) 755-5909 (24/7 Toll-Free USA Phone Support)
- +1. (800) 889-5113 (24/7 Toll-Free Canada Phone Support)
- +61 (290) 372-132 (24/7 Phone Support Australia)
- +44 (120) 925-01-11 (24/7 Phone Support UK)

**User details:**

Login: jelogs@gmail.com

Password: [REDACTED]

**Member's Area:** <http://advancedcleaner.com/members/login.html>



Jessie Logan <jelogs@gmail.com>

# Thank you for your purchase!

1 message

support@advancedcleaner.com  
<support@advancedcleaner.com>  
To: jelogs@gmail.com

Wed, Mar 12,  
2008 at 1:19 PM



**To:** Jessie Logan  
**From:** AdvancedCleaner + Premium  
Support Support Department  
**Subject:** Your advancedcleaner.com  
order

If you have faced any issues to download or install AdvancedCleaner + Premium Support software please kindly use direct link:  
[advancedcleaner.com](http://advancedcleaner.com)

**Dear Jessie Logan,**

Thank you for your order.

**Product:** AdvancedCleaner + Premium Support

**Site:** [advancedcleaner.com](http://advancedcleaner.com)

**Order Billed As:** [supportsw.com](http://supportsw.com) 8007555909

**Order Number:** 6153843

Your Software can be downloaded from [this link](#)

**User name:** [jelogs@gmail.com](mailto:jelogs@gmail.com)

**Password:** Dixie

**BILLING INFORMATION:** Your Charge Description will appear as  
"supportsw.com 8007555909" for the purchase of AdvancedCleaner +  
Premium Support from [advancedcleaner.com](http://advancedcleaner.com) for **64.90 USD**.

For your convenience, we have created a very user-friendly and informative  
[FAQ](#) section, which lists answers to many commonly asked questions. Please  
refer to this section for answers to your questions. And also a guide link for  
Installation, [InstallationGuide](#)

### Extended Download Service

a. Your order is a downloadable product under Extended Download Service from our stores, you are automatically granted a 12 month access in which your purchase can be re-downloaded at any time.

b. Shipping of a Product CD is not available with this offer

If you have any questions or concerns please contact our **Technical Support Center** at [support@advancedcleaner.com](mailto:support@advancedcleaner.com)

**+1. (202) 904-2212 (24/7 Phone Support)**

**+1. (800) 755-5909 (24/7 Toll-Free USA Phone Support)**

**+1. (800) 889-5113 (24/7 Toll-Free Canada Phone Support)**

**+61 (290) 372-132 (24/7 Phone Support Australia)**

**+44 (120) 925-01-11 (24/7 Phone Support UK)**

Please be informed that from now on you have a full access to our Member's Area where you can clarify all the doubts you have regarding usage of your software.

Please allow our support division a reasonable response time. Also, be sure to include your Order Number in the Subject Line with any correspondence.

Warm Regards,

**Staff [advancedcleaner.com](http://advancedcleaner.com)**

[advancedcleaner.com](http://advancedcleaner.com)

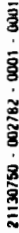
[support@advancedcleaner.com](mailto:support@advancedcleaner.com)

This e-mail is confidential and non-SPAM. If you received this message by mistake, please delete all copies from your system and notify the sender immediately by return e-mail. The sender does not accept liability for any errors or omissions.

Letter content was  
scanned

No threat detected

[advancedcleaner.com](http://advancedcleaner.com)



Payment coupon: Please tear along perforation and return this portion with your payment. Make check or money order payable in U.S. dollars on a U.S. bank to Citibank. Include account number on check or money order. No cash please. Do not staple or tape your check to this coupon.

## PAGE 1 of 1

ello Alexander,

have attached for your review a copy of the test purchase file we have ready to put into our system upon receipt of your final approval. As outlined in our test purchase program (I attached copy of that for you as well) we can only work with US and Canadian consumers and we limit the initial purchase to \$50,000.00 face value to allow us to see how our accounts track.

We took a sampling of the original file Broost sent us that consists of 202 accounts for a total face value of \$50,952. The purchase price, based on the ages of the accounts is as follows;

12 accs >7 <12 @ \$2,935 x .05 = \$147  
157 accs >4 <7 @ \$26,798 x .10 = \$2,680  
173 accs <4 mos @ \$21,220 x .125 = \$2,652

Total remit will be \$5,479.00 Please advise of preferred payment method, .E. ACH, wire transfer, mailing address etc.

One final question that came up is if you have any type of "delivery confirmation" available within your systems.

Can you also please provide us with your phone number as we may need to contact you in the event we have particular customer service issues along the way. My direct telephone number is (419)517-0023 (EST)

Thank you again,

Tony Shula

order ID,cbk date,Email,First,Mid/Last,Last,First Name,Last Name,Login,Address,Zip code,City,State,Phone,Site Name,Transaction Date,CCID,IP,Prod Name,Cost,Purchase Amt

1835959,4/17/2006, [REDACTED],susan,k,ulle,susan [REDACTED],euclid,OH,,winfixer.com,10/8/2005  
14:50, [REDACTED],WinFixer 2005,39.95,  
1878134,4/21/2006, [REDACTED],Ignacio,,Ignacio,Serricchio, [REDACTED],Culver City,CA,,winantispware.com,10/24/2005  
3:41, [REDACTED],WinAntiSpyWare 2005,39.95,  
1887686,5/19/2006, [REDACTED],Donald,Ward,,Donald Ward, [REDACTED],Machesney Park,IL, [REDACTED]  
[REDACTED],winfixer.com,10/27/2005 9:30, [REDACTED],WinFixer 2005,39.95,  
1911862,4/21/2006, [REDACTED],linda,mews,,linda mews, [REDACTED],chapel hill,NC,,winfixer.com,11/3/2005  
18:56, [REDACTED],WinFixer 2005,39.95,  
1966279,4/5/2006, [REDACTED],Marty,L,Peltier,Marty L Peltier, [REDACTED],Warren,MI, [REDACTED],winfixer.com,11/19/2005  
5:10, [REDACTED],WinFixer 2005,39.95,  
1971045,4/21/2006, [REDACTED],JOHN,P,CORTESE,JOHN P CORTESE, [REDACTED]  
[REDACTED],ROCHESTER,NY,,winfixer.com,11/20/2005 11:20, [REDACTED],WinFixer 2005,39.95,  
1985129,4/3/2006, [REDACTED],tim,dahn,,tim dahn, [REDACTED],oceanside,CA,,winfixer.com,11/24/2005  
11:31, [REDACTED],WinFixer 2005,39.95,  
1997424,5/10/2006, [REDACTED],Charlotte,K,Weaver,Charlotte K Weaver, [REDACTED]  
[REDACTED],Corsicana,TX, [REDACTED],winfixer.com,11/27/2005 22:40, [REDACTED],WinFixer 2005,39.95,  
2000398,4/5/2006, [REDACTED],Margaret,,Margaret,Burnham, [REDACTED],Lodi,CA,,winantiviruspro.com,11/28/2005  
18:35, [REDACTED],WinAntiVirus Pro 2006,49.95,  
2020455,4/11/2006, [REDACTED],Allan,hedberg,,Allan hedberg, [REDACTED],MANhasset,NY, [REDACTED]  
[REDACTED],winfixer.com,12/4/2005 5:26, [REDACTED],WinFixer 2005,42,  
2030265,4/7/2006, [REDACTED],Cynthia,M,,Neal,Cynthia M. Neal, [REDACTED],Lomita,CA, [REDACTED],winfixer.com,12/6/2005  
11:32, [REDACTED],WinFixer 2005,39.95,  
2033936,4/5/2006, [REDACTED],sheldon,perl,,sheldon perl, [REDACTED],lawrence,NY, [REDACTED],winfixer.com,12/7/2005  
9:38, [REDACTED],WinFixer 2005,39.95,  
2035313,4/3/2006, [REDACTED],leonora,m,ostermeier,leonora m ostermeier, [REDACTED],richmond hill,NY,1 [REDACTED]  
[REDACTED],winfixer.com,12/7/2005 15:53, [REDACTED],WinFixer 2005,39.95,  
2045076,4/11/2006, [REDACTED],John,M,Kelly,John M Kelly, [REDACTED],Chappaqua,NY,,winfixer.com,12/10/2005  
4:02, [REDACTED],WinFixer 2005,39.95,  
2050999,4/21/2006, [REDACTED],Christopher,C,Festa,Christopher C Festa, [REDACTED],Braintree,MA,,winfixer.com,12/11/2005  
12:41, [REDACTED],WinFixer 2005,39.95,  
2053132,4/5/2006, [REDACTED],Michele,Parsons,,Michele Parsons, [REDACTED],Conklin,NY,,winfixer.com,12/11/2005  
23:26, [REDACTED],WinFixer 2005,39.95,  
2055615,4/5/2006, [REDACTED],Terrance,J,,Moeller,Terrance J. Moeller, [REDACTED],West Point,IA,,winfixer.com,12/12/2005  
13:59, [REDACTED],WinFixer 2005,39.95,  
2060370,4/21/2006, [REDACTED],sharon,rigney,,sharon rigney, [REDACTED],danville,VA, [REDACTED],winfixer.com,12/13/2005  
19:15, [REDACTED],WinFixer 2005,39.95,  
2060390,4/3/2006, [REDACTED],CYNTHIA,,CYNTHIA,CUTTING, [REDACTED],TAUNTON,MA, [REDACTED]  
[REDACTED],winantiviruspro.com,12/13/2005 19:23, [REDACTED],WinAntiVirus Pro 2006,49.95,  
2063165,4/5/2006, [REDACTED],Joan,M,Mangels,Joan M Mangels, [REDACTED],Irvine,CA,,winfixer.com,12/14/2005  
13:17, [REDACTED],WinFixer 2005,39.95,  
2067590,5/2/2006, [REDACTED],patricio,,patricio,abdon, [REDACTED],san diego,CA, [REDACTED],Winantivirus.com,12/15/2005

---

**From:** "Alexandr" <kurbik@innovativemarketing.com.ua>  
**To:** "'Tony Shula'" <tony@crbcompany.com>; "'Tamila'" <tamila@innovativemarketing.com.ua>  
**Sent:** Wednesday, January 17, 2007 9:01 AM  
**Attach:** Sunwell Details.xls  
**Subject:** FW: FW: CRB agency

Hi Tony,

Marc not works for our company any more.  
So please find new bank account information in attachment.

Wire transfer was to wrong bank account and we didn't get the money.

Best regards,  
Alexandr.

-----Original Message-----

**From:** Dmitriy Sancha [mailto:wm@innovativemarketing.com.ua]  
**Sent:** Wednesday, January 17, 2007 2:42 PM  
**To:** 'Alexandr'  
**Subject:** RE: FW: CRB agency

Sunwell's details for this agreement are in attachment.  
Notice, descriptions is necessary for this details.

-----Original Message-----

**From:** Andrew Dzyubenko [mailto:key@innovativemarketing.com.ua]  
**Sent:** Wednesday, January 17, 2007 2:14 PM  
**To:** 'Dmitriy Sancha'  
**Cc:** 'Alexandr'; 'Sam'  
**Subject:** FW: FW: CRB agency

CRB is an agency that we're giving out chargebacks information to,  
and they fight for getting them fixed and pay us .15 cents for each \$1 they  
provide us. For this 11k\$ they have sent, we won't pursue them now, we'll  
get them back other way.

Right now we need to communicate with them, that marc is no longer  
works for us, and that we want to continue working with them, so if they  
have any agreement with marc, request it from them, and resign for our  
corporation, and also provide the new banking details.

Wm, please provide the new corporation/bank account details to  
Kurbik, Kurbik please have the new relations set.

Attachment P

Please, have this resolved:

-----Original Message-----

From: Alexandr [mailto:kurbik@innovativemarketing.com.ua]  
Sent: Wednesday, January 17, 2007 1:49 PM  
To: 'broost'; 'Andrew Dzyubenko'  
Subject: FW: FW: CRB agency

Looks like our money sent to Marc :(

-----Original Message-----

From: Tammy Yoder [mailto:tammy@crbcompany.com]  
Sent: Tuesday, January 16, 2007 8:42 PM  
To: Alexandr  
Cc: Tony  
Subject: Re: FW: CRB agency

Hello Alexandr,  
Tony is at the Internext Expo this week; actually I sent a remit on  
01/04/07 for the last file we received in late December. I trust you got  
it (\$11,375.56)? Could you please forward the new banking info when you  
send the next file?  
Thank you -  
Tammy

> Hi Tony,  
>  
>  
>  
> Our bank account information has changed.  
>  
> Let me know when you plan to send money I'll provide you with account  
> information  
>  
>  
>  
> Best regards,  
>  
> Alexandr  
>  
>  
>  
> \_\_\_\_\_  
> From: Helen [mailto:hp@innovativemarketing.com.ua]  
> Sent: Tuesday, January 16, 2007 11:34 AM  
> To: 'Alexandr Kurbatov'; [fess@imu.kiev.ua](mailto:fess@imu.kiev.ua)  
> Subject: CRB agency

>  
>  
>  
> FYI  
>  
> Today we received a report from Tammy from CRB. The total revenue in this  
> list is about \$8000.  
>  
>  
>  
> Innovative Marketing Ukraine  
>  
> Prykhnych Helen | Return Operations Manager  
>  
> ICQ 205096852 | IRC hp  
>  
> MSN <<mailto:helen4585@hotmail.com>> [helen4585@hotmail.com](mailto:helen4585@hotmail.com)  
>  
> Ext. 2224 | Skype hp\_imu  
>  
> E-mail <<mailto:hp@innovativemarketing.com.ua>> :  
> [hp@innovativemarketing.com.ua](mailto:hp@innovativemarketing.com.ua)  
>  
>  
>  
>

---

CONFIDENTIALITY NOTICE:

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

---

| Payment details for wire         |                                               |
|----------------------------------|-----------------------------------------------|
| Beneficiary:                     | Sunwell Incorporation                         |
| Beneficiary Account:             |                                               |
| Beneficiary Address:             | 5 New Road, P.O. Box 388, Belize City, Belize |
| Beneficiary Bank:                | JSC "Aizkraukles banka"                       |
| Beneficiary Bank Address:        | 23 Elizabets St., Riga, Latvia, LV-1010       |
| Beneficiary Bank SWIFT/BIC/ABA:  | AIZK LV 22                                    |
| Intermediary Account:            |                                               |
| Intermediary Bank:               | AMERICAN EXPRESS BANK, LTD.                   |
| Intermediary Bank Address:       | New York, United States                       |
| Intermediary Bank SWIFT/BIC/ABA: | AEIB US 33                                    |
| Payment description:             | According Agreement BK-12, 01/16/2007         |





Attachment P

Page 306



# James Reno

Tue, 11 Dec 2007 11:37:10 -0500

|                                                                                   |                                   |                                                                                   |                                 |
|-----------------------------------------------------------------------------------|-----------------------------------|-----------------------------------------------------------------------------------|---------------------------------|
|  | Linux Administration<br>(General) |  | Apache 1.3.12<br>Administration |
|  | MySQL 3.23<br>Administration      |  | HTML 3.2                        |

[ BrainBench Transcript ]

## Projects im Involved In:

- ByteHosting Internet Services, LLC  
(Owner)
  - ils.net / InOneSearch.com
  - phpcluster.net - PHP/LAMP  
Clustering Software
  - ByteCenter Web Services, LLC
    - ByteIRC.net IRC Network
- GoAndBitch.com

## Websites I Visit:

- Digitally Imported Radio
- Club977 - The Mix Channel (KMGX)

## Languages I Know:

- PHP (3.x, 4.x, 5.x)
- Perl (4.x, 5.x)
- JavaScript
- HTML (4.x)
- SQL
- Visual Basic (6)
- Bash/SH - Batch (2.x, 3.x)
- TCL
- Basic
- CSS
- English (US)

## My Internet Pages:

These are pages which contain information about me.

- ICANN [view]
- Zabbix Forums [View]
- MySpace [View]

## Software Experience:

- [L]inux (Mandriva Linux)
- [A]pache Webserver
- [M]ysql Database Server
- [P]HP
- Monitoring: Nagios, Zabbix
- UnrealIRCd
- ipsec-tools (racoon)
- eMail Servers: Postfix, qMail, exim
- Shoutcast DNAS
- K Desktop Environment (KDE): 3.x
- Common Unix Printing System (CUPS)
- Telephony Software: Asterisk (1.x)
- WebServers: Apache (1.x, 2.x),  
lighttpd (1.x), NGiNX (0.x), boa,  
thttpd

## Hardware Experience:

- Juniper Routers: M10, M20, M40  
(JunOS)

Attachment Q

### Protocols I Speak:

- HTTP/1.0 & 1.1 (fluent)
- RFC1459 (IRC), 2810,2811,2812,2813 (fluent)
- SMTP/ESMTP (fluent)
- POP3
- IMAP

### Education:

- West Clermont Local: High School Diploma
- ITT Technical Institute: Computer Science/Computer Network Systems

### Technologies:

- Network Cabling:
  - UTP: cat5, cat5e, cat6
  - Optical Fiber: (LH) Simplex, (SX) Multi-Mode
  - Coax
- Network Protocols:
  - Ethernet: 10/100/1000 (UTP/Fiber)
  - Sonet/ATM: OC3, OC12, OC48
  - Wireless: 802.11a/b/g

### Misc. Experience:

- Content Delivery: LimeLight, Akamai

### Interests & Hobbies (beyond computers):

- ATV (4-wheeling)
- WaterCraft (Boating, Seadoos, ect)

- Cisco Systems:
  - Routers: 1600, GSR (IOS)
  - Switches: 2900, 3500 (IOS); 6500 (CatOS)
  - IP-Phones: 7940G, 7960G
- Extreme Networks:
  - Summit: 4, 48i
- Dell:
  - PowerEdge: SC, 1440, 1750, 1850, 1950, 2650, 2950
  - PowerVault: 220S
  - PowerConnect Switches
- Various:
  - Raid Controllers: 3ware, Adaptec, Dell PERC

### Operating Systems:

- Linux:
  - Mandriva: 9.x, 10.x, LE2005, 2006, 2007.x
  - Redhat: 7.x, 9.x
  - CentOS: 3, 4, 5
  - Fedora: Core 2
- BSD:
  - FreeBSD: 3.x, 4.x, 5.x, 6.x
  - NetBSD
  - OpenBSD
- UNIX:
  - Solaris
- Microsoft Windows:
  - 95 (a/b), 98, ME
  - NT4, 2000 (NT 5.0), XP (NT 5.1)
  - 2003 Server (Datacenter Edition)
  - Vista

### Favorites:

- Color: red
- Subject: Science
- Thing-to-do: take things apart

1 Joseph M. Bochner (SBN 147911)  
1259 El Camino Real, PMB 221  
2 Menlo Park, CA 94025  
(650) 575-6590

3 Attorney for Plaintiff  
4 Beatrice Ochoa

(ENDORSED)  
**FILED**  
SEP 29 2006

KIRI TORRE  
Chief Executive Officer/Clerk  
Superior Court of CA County of Santa Clara  
By Sara Batrez DEPUTY

5  
6  
7  
8 SUPERIOR COURT OF THE STATE OF CALIFORNIA  
9 SANTA CLARA COUNTY

10  
11 BEATRICE OCHOA,

12 Plaintiff,

13 vs.

14  
15 MARC J. COHEN and DOES 1 THROUGH  
100,

16 Defendants.  
17

: CASE NO. **106CV072057**

:  
:  
:  
: CLASS ACTION

:  
:  
: COMPLAINT FOR DAMAGES AND  
INJUNCTIVE RELIEF

18 Plaintiff Beatrice Ochoa, for herself and all others similarly situated, complains against  
19 Defendants Marc J. Cohen and Does 1 through 100. Plaintiff's allegations are based upon  
20 information and belief, except as to her own actions, which are based on knowledge. Plaintiff  
21 alleges:  
22

23 INTRODUCTION

24 1. Defendants distribute fraudulent and malicious software under various names, including  
25 without limitation WinFixer, ErrorSafe, WinAntiVirus and WinAntiSpyware (collectively  
26 "Fraudware"). The Fraudware is installed through downloads from dozens of different websites,  
27 including winfixer.com, errorsafe.com and many others. As of 2006, most of Defendants'  
28 websites resolve to Internet Protocol ("IP") addresses at 66.244.254.63 and 66.244.254.177.

1 Because IP addresses can change at any time, discovery may disclose different or additional IP  
2 addresses, without affecting the substance of the allegations here.

3 2. Part and parcel of Defendants' Fraudware conspiracy is the failure to disclose accurate or  
4 valid personal and business names, their falsification of such names, and the use of fictitious  
5 names, all employed to foster ignorance, uncertainty and confusion about Defendants' true  
6 identities and addresses. To accomplish this, Defendants conduct their fraudulent business under  
7 dozens of different Internet domain names, publish false contact information when registering  
8 those domains, and fail to comply with statutes mandating disclosure. The intended and practical  
9 effect is to obscure and to conceal Defendants' identities and whereabouts in furtherance of their  
10 fraud and conspiracy.

11 3. Defendants' Fraudware installs itself either in a "drive by" attack, of which the user may  
12 be unaware, or by displaying fraudulent messages representing that the victim's computer has  
13 already been "infected" with other harmful software. These representations are fraudulent (and  
14 very often flatly false) in that Defendants have designed and intended the Fraudware to report  
15 that the host computer is infected regardless of the truth. The Fraudware then misrepresents that  
16 the victim may repair the purported problem by paying money to Defendants. Victims who  
17 comply are instructed to enter credit card information and to transmit it over the Internet,  
18 whereupon Defendants charge the victims from \$29.95 to \$59.95, depending on the particular  
19 Fraudware title involved. Regardless of precise method or price, Defendants cause the Fraudware  
20 to be downloaded and installed on the victim's computer.

21 4. Defendants' Fraudware hijacks or "redirects" the victim's computer to several websites,  
22 including without limitation VipFares. VipFares sells travel services and ostensibly operates  
23 legitimately, but in fact attracts customers primarily (if not exclusively) through Fraudware  
24 redirects. Because of such hijacking, Plaintiff and the Class lose substantial control over their  
25 computers. Correspondingly, via hijacking Defendants benefit from large amounts of Internet  
26 traffic, commerce and money to which they are not otherwise entitled.

27 5. Fraudware consumes valuable hardware and software resources and hinders computer  
28 performance. Furthermore, Fraudware is not, by its nature, robust, and therefore its installation

1 alone is often enough to cause serious problems including loss of data and usability of the  
2 machine. Nevertheless inexperienced victims may not realize that Fraudware has attacked or  
3 hijacked their computers. Those who do must either spend additional money on a legitimate  
4 computer protection program, or expend many hours of time troubleshooting the problem, or hire  
5 a computer expert, or else simply suffer. In many instances the latter occurs because the  
6 Fraudware is designed to and will reinstall itself upon deletion. With computers having become  
7 useful tools in nearly every facet of personal and professional life, Class-wide economic and  
8 noneconomic damages run high, deep and broad throughout the full spectrum of society.  
9 Regardless how a victim responds, Defendants, through the Fraudware, consciously and  
10 deliberately cause money losses, wasted human and computer resources, and untold misery to  
11 millions of people, including Plaintiff and the Class.

#### 12 13 PARTIES

14 6. Plaintiff Beatrice Ochoa resides in Santa Clara County, California, and purchased  
15 WinFixer on the Internet for \$29.95.

16 7. Defendant Marc J. Cohen ("Cohen") resides in Florida and is the owner and operator of  
17 VipFares. He, and those acting under or with him, designed, produced, control, and distribute the  
18 Fraudware. Cohen personally benefits directly through Fraudware sales, as well as indirectly  
19 through computer hijacking, and all at the expense of Plaintiff and the Class.

20 8. Does 1 through 100 are fictitious names of individuals or companies directly or indirectly  
21 participating with Defendant Cohen in Fraudware creation, distribution, marketing, sales, credit  
22 card processing, telephone response, web hosting, or other unlawful associated activities.  
23 Plaintiff will amend this complaint to allege the true names of the fictitious defendants when  
24 ascertained.

25  
26  
27 Attachment R  
28

CLASS ACTION ALLEGATIONS

9. Plaintiff brings this action on behalf of herself and all others similarly situated. The Class consists of all persons who purchased, received or used any of Defendants' Fraudware programs, including without limitation WinFixer, ErrorSafe, WinAntiVirus and WinAntiSpyware.

10. This Court should certify the Class because:

- a. The Class is extremely numerous, consisting of hundreds of thousands (if not millions) in the United States alone. Joinder is obviously impractical. The Court and counsel can readily ascertain the precise number and identities of absent class members with reference to information in Defendants' possession. While damages per class member are relatively small, aggregate Class damages are large, totaling tens of millions and perhaps more. Discovery and expert testimony at trial will substantiate the amount.
- b. Common questions of law and fact predominate over questions affecting only individual Class members. Without limitation, the common questions include whether Defendants:
  - i. Participated in the Fraudware scheme alleged here;
  - ii. Knew (or should have known) they were harming Plaintiff and the Class;
  - iii. Obtained unauthorized access to computers belonging to Plaintiff and the Class through fraudulent means;
  - iv. Charged the credit cards of Plaintiff and the Class, likewise through fraud;
  - v. Hijacked the computers of Plaintiff and the Class; and
  - vi. Damaged computers belonging to Plaintiff and the Class, causing the monetary and other losses alleged here.
- c. Plaintiff's claims are typical of the Class because, among other things, Defendants caused the Fraudware to install, hijack and damage Plaintiff's computer, and to charge Plaintiff's credit card in the bargain, and all in typical fashion.
- d. Plaintiff, by and through counsel, will fairly and vigorously represent the Class. Plaintiff's interests are consistent with those of absent class members to seek

1 redress for Defendants' wrongs. To that end, Plaintiff has retained counsel who is  
2 zealous, competent and experienced in class and complex litigation, as well as the  
3 subject matter involved.

4 For these reasons, class treatment is far superior to all other means for the fair and efficient  
5 adjudication of this dispute. As a practical matter, the expense and burden of individual litigation  
6 makes it impossible for members of the Class to individually redress the wrongs alleged here. On  
7 the other hand, managing this case as a class action presents no unusual difficulty.

8 11. In addition, the Class should be certified because:

- 9 a. Separate actions by the individual members of the Class would create a risk of  
10 inconsistent adjudication;  
11 b. Separate actions by individual Class members would create a risk of precedential  
12 effect which would substantially impair or impede other Class members' ability to  
13 protect their interests in any separate litigation; and  
14 c. Defendants, through the Fraudware, have acted on grounds generally applicable to  
15 the Class, under circumstances that render class-wide damages and injunctive  
16 relief particularly appropriate.

17  
18 FIRST CAUSE OF ACTION

19 (Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*)

20 12. Plaintiff incorporates by reference the previous allegations.

21 13. Defendants' Fraudware violates the Computer Fraud and Abuse Act, section 1030 of title  
22 18, United States Code, which generally proscribes the knowing or reckless transmission of  
23 damaging software, information, code or commands to a protected computer.

24 14. The computers of Plaintiff and the Class are "protected computers" because they are used  
25 in interstate commerce (i.e. the Internet).

26 15. As a result of Defendants' unlawful conduct, Plaintiff and the Class have been damaged  
27 according to proof at trial.

28 Attachment R

1 16. During the last year, the aggregate harm caused to Plaintiff and the Class far exceeds  
2 \$5,000.

3  
4 SECOND CAUSE OF ACTION

5 (Common Law Fraud)

6 17. Plaintiff incorporates by reference the previous allegations.

7 18. Defendants have knowingly or recklessly engaged in the fraud and deception alleged  
8 above in order to install the Fraudware on computers without their owners' knowledge or lawful  
9 consent, to fraudulently induce Plaintiff and the Class to pay for the Fraudware, and to hijack  
10 their computers.

11 19. Plaintiff and the Class had no knowledge of the falsity and/or incompleteness of  
12 Defendants' misrepresentations or other fraudulent conduct, and therefore reasonably relied to  
13 their detriment as alleged above.

14 20. As a result of Defendants' unlawful conduct, Plaintiff and the Class have been damaged  
15 according to proof at trial.

16 21. Defendants' conduct in perpetuating the fraud and deceptive practices described above is  
17 malicious, willful, wanton and oppressive, or in reckless disregard of the rights of Plaintiff and  
18 the Class, thereby warranting the imposition of punitive damages.

19  
20 THIRD CAUSE OF ACTION

21 (Trespass)

22 22. Plaintiff incorporates by reference the previous allegations.

23 23. By engaging in the acts described above without the authorization of Plaintiff and the  
24 Class, Defendants seized control over the operation of the computers of Plaintiff and the Class,  
25 dispossessing Plaintiff and the Class from use of, access to or control over their computers, and  
26 impairing such computers' use, value, and quality.

27 24. Defendants' acts constitute an intentional interference with the use and enjoyment of the  
28 computers belonging to Plaintiff and the Class.

Attachment R

1 25. As a result of Defendants' unlawful conduct, Plaintiff and the Class have been damaged  
2 according to proof at trial.

3 26. Defendants' trespass was and is malicious, willful, wanton and oppressive, or in reckless  
4 disregard of Plaintiff's rights, thereby warranting the imposition of punitive damages.

5  
6 FOURTH CAUSE OF ACTION

7 (RICO, 18 U.S.C. 1962 *et seq.*)

8 27. Plaintiff incorporates by reference the previous allegations.

9 28. Defendants' participation together in the creation, distribution, marketing, sales, credit  
10 card processing, telephone response and web hosting of Fraudware constitutes a criminal  
11 enterprise in which each participant plays a substantial role. There is probable cause to believe  
12 that Defendant Marc J. Cohen orchestrates and is the principal beneficiary of this conspiracy.

13 29. Fraudware distribution involves the crime of Wire Fraud under section 1343 of title 18,  
14 United States Code, in that Defendants commit their fraud using the Internet as their primary  
15 instrumentality of misinformation, fraud, distribution, sales, hijacking and other unlawful  
16 activities. Defendants' repeated and ongoing wrongful acts comprise a definite and ongoing  
17 pattern of racketeering. Defendants' racketeering unlawfully benefits VipFares and other  
18 websites to which the Fraudware redirects traffic, at the expense of Plaintiff and the Class.

19 30. As a result of Defendants' unlawful conduct, Plaintiff and the Class have been damaged  
20 according to proof at trial.

21  
22 FIFTH CAUSE OF ACTION

23 (Violation of Section 17200 *et seq.* of the California Business & Professions Code)

24 31. Plaintiff incorporates by reference the previous allegations.

25 32. Defendants' Fraudware-related conduct constitutes unfair competition: such conduct  
26 violates numerous state and federal statutes and common law doctrines as alleged above.  
27 Fraudware constitutes an ongoing affront to the conduct of lawful business.

28 33. Defendants' unfair competition will continue unless and until enjoined by this Court.

1 34. As a result of Defendants' unlawful conduct, Plaintiff and the Class have been damaged  
2 according to proof at trial.

3 35. As a direct and proximate result of their unfair competition, Defendants have and will  
4 continue to wrongfully reap profits from Plaintiff and the Class, in an amount to be proved at  
5 trial.

6  
7 SIXTH CAUSE OF ACTION

8 (Violation of California Business & Professions Code § 17538)

9 36. Plaintiff incorporates by reference the previous allegations.

10 37. Defendants' commerce via the Internet violates section 17538(d) ("section 17538") of the  
11 California Business & Professions Code, in that Defendants fail to provide (1) a return and  
12 refund policy; (2) their legal names; and (3) the addresses from which they conduct business.

13 38. As a result of Defendants' unlawful conduct, Plaintiff and the Class have been damaged  
14 according to proof at trial.

15  
16 SEVENTH CAUSE OF ACTION

17 (Common Count—Unjust Enrichment)

18 39. Plaintiff incorporates by reference the previous allegations.

19 40. Defendants had and received monies from Plaintiff and the Class that were intended for  
20 their benefit and use.

21 41. By reason of the acts alleged above, Defendants have been unjustly enriched at the  
22 expense of Plaintiff and the Class.

23 42. Plaintiff and the Class have no adequate remedy at law.

24  
25 PRAYER FOR RELIEF

26 WHEREFORE, Plaintiff prays that this Court enter judgment and orders in favor of herself  
27 and the Class and against Defendants as follows:  
28

- 1 A. Certifying the Class, directing that this case proceed as a class action, and appointing
- 2 Plaintiff as Class Representative and her undersigned attorney as Class Counsel;
- 3 B. Awarding Judgment in favor of Plaintiff and the Class for compensatory damages and/or
- 4 restitution according to proof at trial;
- 5 C. Imposing punitive damages to make an example of and to punish Defendants;
- 6 D. Awarding treble damages under RICO;
- 7 E. Enjoining Defendants from designing, using or distributing Fraudware;
- 8 F. Divesting Defendants of any ownership in any enterprise that at any time benefited from
- 9 the use of the Fraudware, including without limitation VipFares;
- 10 G. Imposing a constructive trust upon any funds or other assets unlawfully obtained through
- 11 Defendants' unlawful conduct;
- 12 H. Providing for a substantial incentive award to Plaintiff for her service as Class
- 13 Representative;
- 14 I. Awarding reasonable attorney fees and costs, as well as pre- and post-judgment interest at
- 15 the legal rate; and
- 16 J. Such other and further relief as this Court deems proper.

17 Dated: September 29, 2006

18   
19 \_\_\_\_\_  
20 Joseph Bochner

**California Superior Courts**

CA Superior - Santa Clara  
(Santa Clara)

**1-06-CV-072057****B. Ochoa Vs M. Cohen****This case was retrieved from the court on Tuesday, November 20, 2007****Header**

Case Number: 1-06-CV-072057

Date Filed: 09/29/2006

Date Full Case Retrieved: 11/20/2007

Status: Post 9/4/2007

Misc: (3038) RICO - Unlimited; Civil

[\[Summary\]](#)[\[Participants\]](#)[\[Proceedings\]](#)[\[Associated Cases\]](#)[\[Calendared Events\]](#)**Summary**

Case Retrieved: 10/06/2006

**Participants****Party**

Bytehosting Internet Services Llc

Defendant

Disposition: CV-BT EntryReqDism-No ADR

James Reno

Defendant

Disposition: CV-BT EntryReqDism-No ADR

Marc J. Cohen

Defendant

Disposition: CV-BT EntryReqDism-No ADR

Beatrice Ochoa

Plaintiff

Disposition: CV-BT EntryReqDism-No ADR

**Attorney**

Joseph M. Bochner

Joseph Bochner Law Office

1259 El Camino Real, Post Mail Box 221

Menlo Park CA 94025

**Proceedings**

| <b>Number</b> | <b>Date</b> | <b>Description</b>              |
|---------------|-------------|---------------------------------|
| 0001-000      | 09/29/2006  | Cv Complaint Filed/Summs Issued |
|               |             | Ruling: None                    |

**Page 318****Attachment R**

Ruling Date: 09/29/2006

For: Beatrice Ochoa / PLT

Against: Marc J. Cohen / DEF

0002-000 09/29/2006

Cv Summons Filed

Ruling: None

Ruling Date: 09/29/2006

For: Beatrice Ochoa / PLT

Against: Marc J. Cohen / DEF

0003-000 10/19/2006

Cv Case Cover Sheet

Ruling: None

Ruling Date: 10/20/2006

For: Beatrice Ochoa / PLT

Against: Marc J. Cohen / DEF

0004-000 02/02/2007

Cv Case Mgmt Statement

Ruling: None

Ruling Date: 02/02/2007

For: Beatrice Ochoa / PLT

0005-000 02/26/2007

Cv 1st Amended Complaint

Ruling: None

Ruling Date: 02/27/2007

For: Beatrice Ochoa / PLT

Against: Marc J. Cohen / DEF

Against: Bytehosting Internet Services Llc / DEF

Against: James Reno / DEF

0006-000 04/06/2007

Cv Case Mgmt Statement

Ruling: None

Ruling Date: 04/06/2007

For: Beatrice Ochoa / PLT

0007-000 09/04/2007

Cv Req: Dismissal, Entire W/O Prej

Ruling: None

Ruling Date: 09/06/2007

For: Beatrice Ochoa / PLT

Against: Marc J. Cohen / DEF

Against: Bytehosting Internet Services Llc / DEF

Against: James Reno / DEF

## Associated Cases

**No Information is Available for this case**

## Calendared Events

| <u>Date</u> | <u>Time</u> | <u>Description</u>                                                                                                                                                            |
|-------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9/20/2007   | 10:02am     | CV OSC:Sanc/Dism purs to 3.110<br>Result Date: 09/04/07<br>Result: Vacated; dismissal filed<br>Result By: K<br>Notice Printed: 06/19/07<br>Reset To: None<br>Reset From: None |
| 6/12/2007   | 10:00am     | CV Further CMC<br>Result Date: 06/19/07<br>Result: Set for OSC re: Dism<br>Result By: C<br>Notice Printed: 04/11/07<br>Reset To: None<br>Reset From: None                     |
| 4/10/2007   | 10:00am     | CV Further CMC<br>Result Date: 04/10/07<br>Result: Set for further CMC<br>Result By: C<br>Notice Printed: 02/15/07<br>Reset To: None<br>Reset From: None                      |
| 2/6/2007    | 01:30pm     | CV CMC-Case Management Conf<br>Result Date: 02/15/07<br>Result: Set for further CMC<br>Result By: C<br>Notice Printed: None<br>Reset To: None<br>Reset From: None             |

Copyright © 2007 LexisNexis CourtLink, Inc. All rights reserved.  
\*\*\* THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY \*\*\*



# Phone Number (DID) Browse for Account ByteHosting Internet Services LLC

Search for  that  Contains  Search Text

Select: All, None

| Number                   |            | DID         | UID  | OID  | AID | Destination | Failover Routing   | Note   | Created   |                     |
|--------------------------|------------|-------------|------|------|-----|-------------|--------------------|--------|-----------|---------------------|
| <input type="checkbox"/> | Edit   Del | 12027470929 | 8725 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000002 | 2007-04-04 19:53:07 |
| <input type="checkbox"/> | Edit   Del | 12029042212 | 8724 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000002 | 2007-04-04 19:52:28 |
| <input type="checkbox"/> | Edit   Del | 12054511916 | 8723 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000002 | 2007-04-04 19:52:03 |
| <input type="checkbox"/> | Edit   Del | 12127960898 | 8722 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000002 | 2007-04-04 19:51:38 |
| <input type="checkbox"/> | Edit   Del | 13108817225 | 8721 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000002 | 2007-04-04 19:51:02 |
| <input type="checkbox"/> | Edit   Del | 15128794683 | 8730 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000002 | 2007-04-04 19:55:08 |
| <input type="checkbox"/> | Edit   Del | 15132861120 | 8704 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-04 01:41:24 |
| <input type="checkbox"/> | Edit   Del | 15132861121 | 8792 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-09 22:40:58 |
| <input type="checkbox"/> | Edit   Del | 15132861122 | 8782 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-09 22:16:43 |
| <input type="checkbox"/> | Edit   Del | 15132861123 | 8898 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-17 23:32:06 |
| <input type="checkbox"/> | Edit   Del | 15132861124 | 8899 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-17 23:32:15 |
| <input type="checkbox"/> | Edit   Del | 15132861125 | 8900 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-17 23:32:25 |
| <input type="checkbox"/> | Edit   Del | 15132861126 | 8783 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-09 22:17:08 |
| <input type="checkbox"/> | Edit   Del | 15132861127 | 8902 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-17 23:32:48 |
| <input type="checkbox"/> | Edit   Del | 15132861128 | 8901 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-17 23:32:55 |
| <input type="checkbox"/> | Edit   Del | 15132861129 | 8903 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-17 23:33:03 |
| <input type="checkbox"/> | Edit   Del | 15132861134 | 8906 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-17 23:33:26 |
| <input type="checkbox"/> | Edit   Del | 15132861135 | 8907 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-17 23:33:26 |
| <input type="checkbox"/> | Edit   Del | 15132861136 | 8905 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-17 23:33:36 |
| <input type="checkbox"/> | Edit   Del | 15132861137 | 8904 | 3621 | 206 | 199         | PSTN Gateway - IAX | Modify | A#0000001 | 2007-04-17 23:33:09 |



# Phone Number (DID) Browse for Account ByteHosting Internet Services LLC

Search for Number



that Contains



Search Text

Go

Reset

Select: All, None

| Number                                          | DID  | UID  | OID | AID | Destination        | Fallover Routing | Note     | Created                                                    |
|-------------------------------------------------|------|------|-----|-----|--------------------|------------------|----------|------------------------------------------------------------|
| <input type="checkbox"/> Edit   Del 15132861138 | 8784 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000001 | <input type="button" value="UFO RTE"/> 2007-04-09 22:17:28 |
| <input type="checkbox"/> Edit   Del 15132971592 | 8781 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000001 | <input type="button" value="UFO RTE"/> 2007-04-09 22:16:16 |
| <input type="checkbox"/> Edit   Del 15132971597 | 8896 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000001 | <input type="button" value="UFO RTE"/> 2007-04-17 23:31:40 |
| <input type="checkbox"/> Edit   Del 15132971598 | 8897 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000001 | <input type="button" value="UFO RTE"/> 2007-04-17 23:31:55 |
| <input type="checkbox"/> Edit   Del 15132971599 | 8786 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000001 | <input type="button" value="UFO RTE"/> 2007-04-09 22:18:19 |
| <input type="checkbox"/> Edit   Del 15132971900 | 8785 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000001 | <input type="button" value="UFO RTE"/> 2007-04-09 22:17:53 |
| <input type="checkbox"/> Edit   Del 15132971901 | 8895 | 3621 | 206 | 199 | PSTN Gateway - SIP | Modify           | A#000001 | <input type="button" value="UFO RTE"/> 2007-04-17 23:31:25 |
| <input type="checkbox"/> Edit   Del 15136850032 | 8705 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000001 | <input type="button" value="UFO RTE"/> 2007-04-04 02:59:56 |
| <input type="checkbox"/> Edit   Del 18002183005 | 8729 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000001 | <input type="button" value="UFO RTE"/> 2007-04-04 19:54:41 |
| <input type="checkbox"/> Edit   Del 18004308969 | 8728 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 | <input type="button" value="UFO RTE"/> 2007-04-04 19:54:24 |
| <input type="checkbox"/> Edit   Del 18004313496 | 8727 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 | <input type="button" value="UFO RTE"/> 2007-04-04 19:54:07 |
| <input type="checkbox"/> Edit   Del 18004406314 | 9481 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 | <input type="button" value="UFO RTE"/> 2007-05-18 15:29:11 |
| <input type="checkbox"/> Edit   Del 18004598084 | 8726 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 | <input type="button" value="UFO RTE"/> 2007-04-04 19:53:45 |
| <input type="checkbox"/> Edit   Del 18004671077 | 8735 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 | <input type="button" value="UFO RTE"/> 2007-04-04 19:58:10 |
| <input type="checkbox"/> Edit   Del 18004707749 | 8734 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 | <input type="button" value="UFO RTE"/> 2007-04-04 19:57:41 |
| <input type="checkbox"/> Edit   Del 18004710735 | 9074 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 | <input type="button" value="UFO RTE"/> 2007-04-25 17:10:42 |
| <input type="checkbox"/> Edit   Del 18004908287 | 8791 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000003 | <input type="button" value="UFO RTE"/> 2007-04-09 22:21:17 |
| <input type="checkbox"/> Edit   Del 18005253796 | 8787 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000001 | <input type="button" value="UFO RTE"/> 2007-04-09 22:19:30 |
| <input type="checkbox"/> Edit   Del 18005562544 | 8894 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000001 | <input type="button" value="UFO RTE"/> 2007-04-17 23:31:07 |
| <input type="checkbox"/> Edit   Del 18006083716 | 8733 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 | <input type="button" value="UFO RTE"/> 2007-04-04 19:57:20 |

Records 21 - 40 of 57

Attachment S

Page 323

Previous 20 | Next 20 | Show All

# Phone Number (DID) Browse for Account ByteHosting Internet Services LLC

Search for  Number  that  Contains  Search Text

Select: All , None

| Number A                                        | DID   | UID  | OID | AID | Destination        | Fallover Routing | Note                                           | Created             |
|-------------------------------------------------|-------|------|-----|-----|--------------------|------------------|------------------------------------------------|---------------------|
| <input type="checkbox"/> Edit   Del 18006206698 | 8790  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000003 <input type="button" value="UPDATE"/> | 2007-04-09 22:21:08 |
| <input type="checkbox"/> Edit   Del 18006264217 | 8873  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-16 00:28:26 |
| <input type="checkbox"/> Edit   Del 18007197144 | 8871  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-16 00:23:21 |
| <input type="checkbox"/> Edit   Del 18007555909 | 8720  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-04 19:36:56 |
| <input type="checkbox"/> Edit   Del 18008308929 | 8788  | 3621 | 206 | 199 | PSTN Gateway - IAX | tel:15132602320  | A#000001 <input type="button" value="UPDATE"/> | 2007-04-09 22:20:09 |
| <input type="checkbox"/> Edit   Del 18008895113 | 8732  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-04 19:56:55 |
| <input type="checkbox"/> Edit   Del 18009765708 | 8731  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-04 19:56:27 |
| <input type="checkbox"/> Edit   Del 18009840534 | 8789  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000003 <input type="button" value="UPDATE"/> | 2007-04-09 22:20:44 |
| <input type="checkbox"/> Edit   Del 18665159316 | 8875  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-16 00:31:42 |
| <input type="checkbox"/> Edit   Del 18668946192 | 8780  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000001 <input type="button" value="UPDATE"/> | 2007-04-09 22:11:36 |
| <input type="checkbox"/> Edit   Del 18773887229 | 11317 | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000005 <input type="button" value="UPDATE"/> | 2007-10-01 10:43:22 |
| <input type="checkbox"/> Edit   Del 18774055223 | 8739  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-04 20:00:00 |
| <input type="checkbox"/> Edit   Del 18774055229 | 8738  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-04 19:59:29 |
| <input type="checkbox"/> Edit   Del 18774204692 | 8737  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-04 19:59:10 |
| <input type="checkbox"/> Edit   Del 18778104127 | 8874  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-16 00:29:48 |
| <input type="checkbox"/> Edit   Del 18778717412 | 8872  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-16 00:26:21 |
| <input type="checkbox"/> Edit   Del 19497432072 | 8736  | 3621 | 206 | 199 | PSTN Gateway - IAX | Modify           | A#000002 <input type="button" value="UPDATE"/> | 2007-04-04 19:58:49 |

Records 41 - 57 of 57

Previous 20 | Next 20 | Show All

---

**From:** "Cathy" <cathy.walton@winsoftware.com>  
**To:** "Tammy Yoder" <tammy@crbcompany.com>  
**Cc:** "Tony Shula" <tony@crbcompany.com>  
**Sent:** Friday, January 26, 2007 1:27 PM  
**Subject:** How to Handle CRB Customers

Tammy,  
I think CRB Reps can also use this below:

So the future policy that should be implemented on ALL AREAS of customer support are like:

**IN ALL CASES A PROPER REPLY:**

"Sorry sir/mam, your account has been turned over to collections due to non-payment. You need to resolve any issues with the collection agency CRB, you can contact them at 1800xxxxx"

----

**Q: I paid my bill via credit card, but a did a dispute, why did you forward my order to a collections agency?**

A: When you order something with your credit card you are AUTHORIZING us as a merchant to electronically debit your card. When you perform a dispute you inform/request your charge to be reversed - much like a STOP PAYMENT with a check -- This does NOT automatically cancel your order, it simply reverses your payment, which results in a order without a payment -- Your money is still due in which you have not paid. Because you have not paid your account has been turned over to collections.

**Q: I received a letter from CRB, who is CRB?**

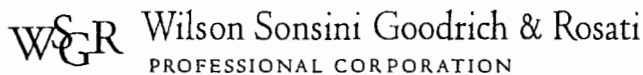
A: Because of NON-PAYMENT on your account, we have turned your account over to collections. CRB is a collection agency acting on our behalf to collect the money in which you owe us.

**Q: This is fraud, im reporting you too....**

A: If you did not place the order or submit your information to us, that is fraud. Us turning you over to a collection agency to collect on a debt in which you owe is not, that is collections. If you did not place the order we can launch a fraud investigation. To launch a fraud investigation it may require you to file a police report on the alleged fraud charges in which the police will ask you certain questions under penalty of perjury (lying to the cops). If you want to launch a fraud investigation I can set your order to fraud and open a case, generally this process will take 4-6 weeks and can take up-to 2 months before the money is returned.

***Remember, we DO NOT talk to the customer, we do NOT help them with customer support, BUT inform them, that "as soon as they pay their bill, we CAN and would be WILLING to do so.***

Regards,  
~James



1700 K Street, NW, Fifth Floor  
Washington, D.C. 20006-3817

PHONE 202.973.8800  
FAX 202.973.8899

[www.wsgr.com](http://www.wsgr.com)

November 14, 2007

**FOIA CONFIDENTIAL TREATMENT**  
**REQUESTED**

**By Federal Express**

Sheryl Drexler  
Investigator  
Federal Trade Commission  
600 Pennsylvania Ave., NW, H-286  
Washington, DC 20580

Re: Limelight Response to Civil Investigative Demand

Dear Ms. Drexler:

Please find enclosed responses with references to documents believed to be responsive to the civil investigative demand ("CID") we received on behalf of our client, Limelight Networks, Inc. (the "Company"), issued on November 5, 2007. The Company is responding and producing these documents pursuant to conversations between the Staff and our attorney, Gerard Stegmaier of the firm Wilson Sonsini Goodrich & Rosati.

**Request:**

Relating to the customer(s) or subscriber(s) associated with the following IP addresses, ULR and/or identifier:

- A. 208.111.153.244 on October 23, 2007 at 4:18:38 PM ET
- B. 208.111.148.137 on October 23, 2007 at 11:03:32 AM ET
- C. Setuphost.vo.llnwd.net
- D. SetUpAHost

And any other account(s) held by the same customer(s) or subscriber(s), please produce the following information during the applicable time period:

1. Name;

Wilson Sonsini Goodrich & Rosati  
PROFESSIONAL CORPORATION

Sheryl Drexler  
November 14, 2007  
Page 2

2. Address;
3. Length of service (including start date) and types of service utilized;
4. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
5. Means and source of payment for such service (including any credit card or bank account number).

**Response:**

The Company's customer is:

Setup A Host, Inc.  
356 Ontario Street  
Suite 301  
Stratford, ON N5A 7X6

The contact information for the Company's customer was last updated on September 27, 2007. Limelight's billing contact is: Julia Shields. The email address the Company has on file for reaching her is: [smile@setupahost.net](mailto:smile@setupahost.net). The sales contact is: James Reno. The Company has the following contact information for Mr. Reno. Email: [james@setupahost.net](mailto:james@setupahost.net) Telephone: 513-685-0032 ext 4501.

The customer has had a billing account with Limelight since August of 2005. Under the current contract between the Company and the customer, the customer is obligated to purchase the following:

ContentEdge CDN Solutions 100 Mbps at \$75.00 per Mbps. \$7,500.00  
Burstable Rate is at \$75.00 per Mbps.  
LUX reporting Package No Charge.

Payments are received via wire transfer under Sunwell and the last payment was on 8/23/2007 with the following detail information:

Detail –  
WT FED#00770 AIZKRAUKLES BANKA  
ORG=SUNWELL INCORPERATED SRF #2433200235JS TRN#070823015992

Wilson Sonsini Goodrich & Rosati  
PROFESSIONAL CORPORATION

Sheryl Drexler  
November 14, 2007  
Page 3

Additionally, we have attached several documents which we believe to be responsive to the CID. These documents have a Bates Range of LLNW-0001 – LLNW-0023.

Through its document production, any subsequent productions, and this correspondence the Company does not, and does not intend to, waive any attorney-client privilege or any other applicable privilege. At the conclusion of the Commission's investigation, the Company requests the return of the enclosed documents and any other materials that the Company provides to the Commission.

The Company also requests that the Commission provide confidential and nonpublic treatment under the Freedom of Information Act ("FOIA") to this letter and the information contained within it. Likewise, we request that the Commission treat the following related materials, in their entirety, as confidential and nonpublic matters under FOIA:

- all prior and subsequent correspondence regarding the Staff's inquiry; and
- any memoranda, notes, transcripts, or other writings made by or at the direction of any Commission employee (or any other government agency) that incorporate, include, refer, or relate to the documents or the information contained within the documents.

Without excluding other grounds, the Company requests confidential treatment based on business confidentiality and personal privacy and because the Company has provided the materials requested pursuant to a confidential, nonpublic investigation. 5 U.S.C. §§ 552 (b)(4) and (7); 16 C.F.R. §§ 4.10(a)(8) and (9). In accordance with the Commission's regulations, we also request that the Company receive notification and the opportunity to contest disclosure of this letter, any of the enclosed documents, any information contained within the documents, or any of the above-described related materials, if the materials are ever the subject of a FOIA request. 16 C.F.R. § 4.10(d).

The address and telephone number for notification is:

Gerard M. Stegmaier  
Wilson, Sonsini Goodrich & Rosati  
1700 K Street, NW, Fifth Floor  
Washington, DC 20006  
Email: [gstegmaier@wsgr.com](mailto:gstegmaier@wsgr.com)  
Telephone: 202-973-8809

Wilson Sonsini Goodrich & Rosati  
PROFESSIONAL CORPORATION

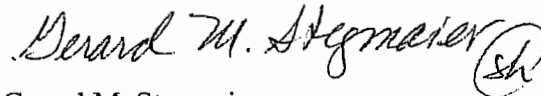
Sheryl Drexler  
November 14, 2007  
Page 4

Also in accordance with Commission regulations, if the Commission tentatively determines that confidential treatment is not warranted with respect to any materials for which the Company has requested confidential treatment, then we request that the Commission notify the Company at least ten days before any intended release of the materials so that the Company may pursue any available remedies, if necessary or appropriate. 16 C.F.R. § 4.10(e).

If you have any questions concerning this matter, please feel free to contact me at 202-973-8809.

Sincerely,

WILSON SONSINI GOODRICH & ROSATI  
Professional Corporation

A handwritten signature in cursive script, reading "Gerard M. Stegmaier", followed by a circular stamp containing the letters "sh".

Gerard M. Stegmaier

Enclosure



Limelight Networks, Inc.  
2220 W. 14th Street  
Tempe, AZ 85281  
(602) 850-5079

# Statement

Statement Date: 11/13/2007

SetupAHost, Inc.  
356 Ontario Street  
Suite 301  
Stratford, ON N5A 7X6

Customer Number: 0805014

Contact: Claudio Santos

| Date      | Reference  | Description             | Charge    | Credit    | Balance |
|-----------|------------|-------------------------|-----------|-----------|---------|
| 11/1/2005 | 0000567-IN | 080500141105            | 1,875.00  |           |         |
| 1/17/2006 |            | Payment Ref: 011706WT   |           | 1,875.00  | 0.00    |
| 12/1/2005 | 0000911-IN | 080500141205            | 4,572.50  |           |         |
| 1/17/2006 |            | Payment Ref: 011706WT   |           | 3,501.25  |         |
| 8/1/2006  |            | Payment Ref: WIRE080106 |           | 1,071.25  | 0.00    |
| 1/1/2006  | 0002595-IN | 080500140106            | 5,376.25  |           |         |
| 8/1/2006  |            | Payment Ref: WIRE080106 |           | 5,376.25  | 0.00    |
| 2/6/2006  | 0003596-IN | 080500140206            | 5,681.25  |           |         |
| 2/22/2006 |            | Payment Ref: 022206WT   |           | 5,681.25  | 0.00    |
| 3/6/2006  | 0010994-IN |                         | 5,038.75  |           |         |
| 3/28/2006 |            | Payment Ref: WIRE032806 |           | 5,038.75  | 0.00    |
| 4/7/2006  | 0012079-IN |                         | 5,806.25  |           |         |
| 5/25/2006 |            | Payment Ref: WIRE052506 |           | 5,806.25  | 0.00    |
| 5/4/2006  | 0013416-IN |                         | 15,607.50 |           |         |
| 5/25/2006 |            | Payment Ref: WIRE052506 |           | 15,607.50 | 0.00    |
| 6/8/2006  | 0014592-IN |                         | 7,500.00  |           |         |
| 8/1/2006  |            | Payment Ref: WIRE080106 |           | 7,500.00  | 0.00    |
| 7/10/2006 | 0015402-IN |                         | 8,225.00  |           |         |
| 8/1/2006  |            | Payment Ref: WIRE080106 |           | 1,487.50  |         |
| 4/25/2007 |            | Payment Ref: WIRE042507 |           | 6,737.50  | 0.00    |
| 8/9/2006  | 0017871-IN |                         | 7,500.00  |           |         |
| 10/4/2006 |            | Payment Ref: WIRE100206 |           | 7,500.00  | 0.00    |
| 9/8/2006  | 0019404-IN |                         | 9,456.00  |           |         |
| 10/4/2006 |            | Payment Ref: WIRE100206 |           | 9,456.00  | 0.00    |
| 10/6/2006 | 0021200-IN |                         | 8,637.00  |           |         |
| 12/7/2006 |            | Payment Ref: WIRE120706 |           | 8,637.00  | 0.00    |
| 11/8/2006 | 0022964-IN |                         | 11,002.50 |           |         |
| 12/7/2006 |            | Payment Ref: WIRE120706 |           | 11,002.50 | 0.00    |
| 12/7/2006 | 0023798-IN |                         | 10,497.75 |           |         |
| 4/25/2007 |            | Payment Ref: WIRE042507 |           | 10,497.75 | 0.00    |
| 1/10/2007 | 0024775-IN |                         | 11,093.25 |           |         |

Continued

\*\*\* THIS IS LINE ONE OF THE STANDARD MESSAGE \*\*\*

\*\*\* THIS IS LINE TWO OF THE STANDARD MESSAGE \*\*\*

Attachment U

Confidential Treatment  
Requested by Limelight  
Networks, Inc.



Limelight Networks, Inc.  
2220 W. 14th Street  
Tempe, AZ 85281  
(602) 850-5079

## Statement

Statement Date: 11/13/2007

Customer Number: 0805014

SetupAHost, Inc.  
356 Ontario Street  
Suite 301  
Stratford, ON N5A 7X6

Contact: Claudio Santos

| Date       | Reference  | Description             | Charge    | Credit    | Balance   |
|------------|------------|-------------------------|-----------|-----------|-----------|
| 2/15/2007  |            | Payment Ref: WIRE021507 |           | 11,093.25 | 0.00      |
| 2/8/2007   | 0026592-IN |                         | 10,263.00 |           |           |
| 4/25/2007  |            | Payment Ref: WIRE042507 |           | 10,263.00 | 0.00      |
| 3/9/2007   | 0027546-IN |                         | 10,464.75 |           |           |
| 4/25/2007  |            | Payment Ref: WIRE042507 |           | 10,464.75 | 0.00      |
| 4/9/2007   | 0029542-IN |                         | 9,634.50  |           |           |
| 4/25/2007  |            | Payment Ref: WIRE042507 |           | 9,634.50  | 0.00      |
| 5/9/2007   | 0031508-IN |                         | 12,301.50 |           |           |
| 8/27/2007  |            | Payment Ref: WIRE082307 |           | 12,301.50 | 0.00      |
| 6/12/2007  | 0033402-IN |                         | 29,335.50 |           |           |
| 6/26/2007  |            | Payment Ref: WIRE062507 |           | 29,335.50 | 0.00      |
| 7/12/2007  | 0034603-IN |                         | 28,804.50 |           |           |
| 9/7/2007   |            | Payment Ref: WIRE090707 |           | 28,804.50 | 0.00      |
| 8/10/2007  | 0035820-IN |                         | 20,211.75 |           |           |
| 8/27/2007  |            | Payment Ref: WIRE082307 |           | 20,211.75 | 0.00      |
| 9/12/2007  | 0037055-IN |                         | 29,875.50 |           | 29,875.50 |
| 10/12/2007 | 0038341-IN |                         | 29,766.75 |           | 29,766.75 |

Total: 59,642.25

| Current   | 30 Days   | 60 Days | 90 Days | 120 Days | Balance Due |
|-----------|-----------|---------|---------|----------|-------------|
| 29,766.75 | 29,875.50 | 0.00    | 0.00    | 0.00     | 59,642.25   |

\*\*\* THIS IS LINE ONE OF THE STANDARD MESSAGE \*\*\*

\*\*\* THIS IS LINE TWO OF THE STANDARD MESSAGE \*\*\*

Just an over-sight? We would appreciate bringing  
your account current. Thanks for your business.

Confidential Treatment  
Requested by Limelight  
Networks, Inc.

**Accounts Receivable Invoice History Report**  
**Sorted by Invoice Number**
**Limelight Networks, Inc. (LLN)**

| Invoice Number   | Invoice Date                   | Source | Customer Number | Name                  | Salesperson Number |
|------------------|--------------------------------|--------|-----------------|-----------------------|--------------------|
| 0000567          | INV 11/1/2005                  | A/R    | 0805014         | SetupAHost, Inc.      | 0207               |
| <b>Item Code</b> | <b>Description</b>             |        | <b>Quantity</b> | <b>Unit Price</b>     | <b>Extension</b>   |
| BB               | 2005 Inv. Bal. from Peachtree  |        |                 |                       | 1,875.00           |
|                  |                                |        |                 | <b>Invoice Total:</b> | 1,875.00           |
| 0000911          | INV 12/1/2005                  | A/R    | 0805014         | SetupAHost, Inc.      | 0207               |
| <b>Item Code</b> | <b>Description</b>             |        | <b>Quantity</b> | <b>Unit Price</b>     | <b>Extension</b>   |
| BB               | 2005 Inv. Bal. from Peachtree  |        |                 |                       | 4,572.50           |
|                  |                                |        |                 | <b>Invoice Total:</b> | 4,572.50           |
| 0002595          | INV 1/1/2006                   | A/R    | 0805014         | SetupAHost, Inc.      | 0207               |
| <b>Item Code</b> | <b>Description</b>             |        | <b>Quantity</b> | <b>Unit Price</b>     | <b>Extension</b>   |
| CDNTRANS01       | ContentEdge Commitment         |        | 15.000          | 125.000               | 1,875.00           |
| CDNTRANSOC01     | ContentEdge Usage Over Commit  |        | 28.010          | 125.000               | 3,501.25           |
| STOR01           | Data Storage Solution          |        | 0.000           | 0.000                 | 0.00               |
| STOROC01         | Data Storage Solution Over     |        | 0.000           | 0.000                 | 0.00               |
| REP01            | LUX Customer Reports           |        | 1.000           | 250.000               | 250.00             |
| REP01            | LUX Customer Reports           |        | 1.000-          | 250.000               | 250.00-            |
|                  |                                |        |                 | <b>Invoice Total:</b> | 5,376.25           |
| 0003596          | INV 2/6/2006                   | A/R    | 0805014         | SetupAHost, Inc.      | 0207               |
| <b>Item Code</b> | <b>Description</b>             |        | <b>Quantity</b> | <b>Unit Price</b>     | <b>Extension</b>   |
| CDNTRANS01       | ContentEdge Commitment         |        | 15.000          | 125.000               | 1,875.00           |
| CDNTRANSOC01     | ContentEdge Usage Over Commit  |        | 30.450          | 125.000               | 3,806.25           |
| STOR01           | Data Storage Solution          |        | 0.000           | 0.000                 | 0.00               |
| STOROC01         | Data Storage Solution Over     |        | 0.000           | 0.000                 | 0.00               |
| REP01            | LUX Customer Reports           |        | 1.000           | 250.000               | 250.00             |
| REP01            | LUX Customer Reports           |        | 1.000-          | 250.000               | 250.00-            |
|                  |                                |        |                 | <b>Invoice Total:</b> | 5,681.25           |
| 0010994          | INV 3/6/2006                   | A/R    | 0805014         | SetupAHost, Inc.      | 0207               |
| <b>Item Code</b> | <b>Description</b>             |        | <b>Quantity</b> | <b>Unit Price</b>     | <b>Extension</b>   |
| CDNTRANS01       | ContentEdge Commitment Current |        | 15.000          | 125.000               | 1,875.00           |
| CDNTRANSOC01     | ContentEdge Usage Over Commitm |        | 25.310          | 125.000               | 3,163.75           |
| REP01            | LUX Customer Reports           |        | 1.000           | 250.000               | 250.00             |
| REP01            | LUX Customer Reports           |        | 1.000-          | 250.000               | 250.00-            |
| STOR01           | Data Storage Solution Current  |        | 0.000           | 0.000                 | 0.00               |
| STOROC01         | Data Storage Solution Usage Ov |        | 0.000           | 0.000                 | 0.00               |
|                  |                                |        |                 | <b>Invoice Total:</b> | 5,038.75           |
| 0012079          | INV 4/7/2006                   | A/R    | 0805014         | SetupAHost, Inc.      | 0207               |
| <b>Item Code</b> | <b>Description</b>             |        | <b>Quantity</b> | <b>Unit Price</b>     | <b>Extension</b>   |
| CDNTRANS01       | ContentEdge Commitment Current |        | 15.000          | 125.000               | 1,875.00           |
| CDNTRANSOC01     | ContentEdge Usage Over Commitm |        | 31.450          | 125.000               | 3,931.25           |
| REP01            | LUX Customer Reports           |        | 1.000           | 250.000               | 250.00             |
| REP01            | LUX Customer Reports           |        | 1.000-          | 250.000               | 250.00-            |
| STOR01           | Data Storage Solution Current  |        | 0.000           | 0.000                 | 0.00               |
| STOROC01         | Data Storage Solution Usage Ov |        | 0.000           | 0.000                 | 0.00               |
|                  |                                |        |                 | <b>Invoice Total:</b> | 5,806.25           |
| 0013416          | INV 5/4/2006                   | A/R    | 0805014         | SetupAHost, Inc.      | 0207               |
| <b>Item Code</b> | <b>Description</b>             |        | <b>Quantity</b> | <b>Unit Price</b>     | <b>Extension</b>   |
| CDNTRANS01       | ContentEdge Commitment Current |        | 15.000          | 125.000               | 1,875.00           |
| CDNTRANSOC01     | ContentEdge Usage Over Commitm |        | 109.860         | 125.000               | 13,732.50          |
| REP01            | LUX Customer Reports           |        | 1.000           | 250.000               | 250.00             |
| REP01            | LUX Customer Reports           |        | 1.000-          | 250.000               | 250.00-            |
| STOR01           | Data Storage Solution Current  |        | 0.000           | 0.000                 | 0.00               |
| STOROC01         | Data Storage Solution Usage Ov |        | 0.000           | 0.000                 | 0.00               |
|                  |                                |        |                 | <b>Invoice Total:</b> | 15,607.50          |
| 0014592          | INV 6/8/2006                   | A/R    | 0805014         | SetupAHost, Inc.      | 0207               |
| <b>Item Code</b> | <b>Description</b>             |        | <b>Quantity</b> | <b>Unit Price</b>     | <b>Extension</b>   |
| CDNTRANS01       | ContentEdge Commitment Current |        | 100.000         | 75.000                | 7,500.00           |
| CDNTRANSOC01     | ContentEdge Usage Over Commitm |        | 0.000           | 0.000                 | 0.00               |
| REP01            | LUX Customer Reports           |        | 1.000           | 250.000               | 250.00             |
| REP01            | LUX Customer Reports           |        | 1.000-          | 250.000               | 250.00-            |

Run Date: 11/13/2007 9:56:14AM

Page: 1

A/R Date: 11/13/2007

User Logon: James

**Accounts Receivable Invoice History Report**  
**Sorted by Invoice Number**
**Limelight Networks, Inc. (LLN)**

| Invoice Number | Invoice Date                   | Source    | Customer Number | Name    | Salesperson Number |                |            |           |
|----------------|--------------------------------|-----------|-----------------|---------|--------------------|----------------|------------|-----------|
| STOR01         |                                |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
| STOROC01       |                                |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
|                |                                |           |                 |         |                    | Invoice Total: | 7,500.00   |           |
| 0015402        | INV                            | 7/10/2006 | A/R             | 0805014 | SetupAHost, Inc.   | 0207           |            |           |
| Item Code      | Description                    |           |                 |         |                    | Quantity       | Unit Price | Extension |
| CDNTRANS01     | ContentEdge Commitment Current |           |                 |         |                    | 100.000        | 75.000     | 7,500.00  |
| CDNTRANSOC01   | ContentEdge Usage Over Commitm |           |                 |         |                    | 5.800          | 125.000    | 725.00    |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000          | 250.000    | 250.00    |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000-         | 250.000    | 250.00-   |
| STOR01         | Data Storage Solution Current  |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
| STOROC01       | Data Storage Solution Usage Ov |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
|                |                                |           |                 |         |                    | Invoice Total: | 8,225.00   |           |
| 0017871        | INV                            | 8/9/2006  | A/R             | 0805014 | SetupAHost, Inc.   | 0207           |            |           |
| Item Code      | Description                    |           |                 |         |                    | Quantity       | Unit Price | Extension |
| CDNTRANS01     | ContentEdge Commitment Current |           |                 |         |                    | 100.000        | 75.000     | 7,500.00  |
| CDNTRANSOC01   | ContentEdge Usage Over Commitm |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000          | 250.000    | 250.00    |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000-         | 250.000    | 250.00-   |
| STOR01         | Data Storage Solution Current  |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
| STOROC01       | Data Storage Solution Usage Ov |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
|                |                                |           |                 |         |                    | Invoice Total: | 7,500.00   |           |
| 0019404        | INV                            | 9/8/2006  | A/R             | 0805014 | SetupAHost, Inc.   | 0207           |            |           |
| Item Code      | Description                    |           |                 |         |                    | Quantity       | Unit Price | Extension |
| CDNTRANS01     | ContentEdge Commitment Current |           |                 |         |                    | 100.000        | 75.000     | 7,500.00  |
| CDNTRANSOC01   | ContentEdge Usage Over Commitm |           |                 |         |                    | 26.080         | 75.000     | 1,956.00  |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000          | 250.000    | 250.00    |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000-         | 250.000    | 250.00-   |
| STOR01         | Data Storage Solution Current  |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
| STOROC01       | Data Storage Solution Usage Ov |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
|                |                                |           |                 |         |                    | Invoice Total: | 9,456.00   |           |
| 0021200        | INV                            | 10/6/2006 | A/R             | 0805014 | SetupAHost, Inc.   | 0207           |            |           |
| Item Code      | Description                    |           |                 |         |                    | Quantity       | Unit Price | Extension |
| CDNTRANS01     | ContentEdge Commitment Current |           |                 |         |                    | 100.000        | 75.000     | 7,500.00  |
| CDNTRANSOC01   | ContentEdge Usage Over Commitm |           |                 |         |                    | 15.160         | 75.000     | 1,137.00  |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000          | 250.000    | 250.00    |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000-         | 250.000    | 250.00-   |
| STOR01         | Data Storage Solution Current  |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
| STOROC01       | Data Storage Solution Usage Ov |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
|                |                                |           |                 |         |                    | Invoice Total: | 8,637.00   |           |
| 0022964        | INV                            | 11/8/2006 | A/R             | 0805014 | SetupAHost, Inc.   | 0207           |            |           |
| Item Code      | Description                    |           |                 |         |                    | Quantity       | Unit Price | Extension |
| CDNTRANS01     | ContentEdge Commitment Current |           |                 |         |                    | 100.000        | 75.000     | 7,500.00  |
| CDNTRANSOC01   | ContentEdge Usage Over Commitm |           |                 |         |                    | 46.700         | 75.000     | 3,502.50  |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000          | 250.000    | 250.00    |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000-         | 250.000    | 250.00-   |
| STOR01         | Data Storage Solution Current  |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
| STOROC01       | Data Storage Solution Usage Ov |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
|                |                                |           |                 |         |                    | Invoice Total: | 11,002.50  |           |
| 0023798        | INV                            | 12/7/2006 | A/R             | 0805014 | SetupAHost, Inc.   | 0207           |            |           |
| Item Code      | Description                    |           |                 |         |                    | Quantity       | Unit Price | Extension |
| CDNTRANS01     | ContentEdge Commitment Current |           |                 |         |                    | 100.000        | 75.000     | 7,500.00  |
| CDNTRANSOC01   | ContentEdge Usage Over Commitm |           |                 |         |                    | 39.970         | 75.000     | 2,997.75  |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000          | 250.000    | 250.00    |
| REP01          | LUX Customer Reports           |           |                 |         |                    | 1.000-         | 250.000    | 250.00-   |
| STOR01         | Data Storage Solution Current  |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
| STOROC01       | Data Storage Solution Usage Ov |           |                 |         |                    | 0.000          | 0.000      | 0.00      |
|                |                                |           |                 |         |                    | Invoice Total: | 10,497.75  |           |
| 0024775        | INV                            | 1/10/2007 | A/R             | 0805014 | SetupAHost, Inc.   | 0207           |            |           |
| Item Code      | Description                    |           |                 |         |                    | Quantity       | Unit Price | Extension |

Run Date: 11/13/2007 9:56:14AM

Page: 2

A/R Date: 11/13/2007

User Logon: James

**Accounts Receivable Invoice History Report**  
**Sorted by Invoice Number**
**Limelight Networks, Inc. (LLN)**

| Invoice Number | Invoice Date                   | Source                         | Customer Number | Name    | Salesperson Number |                      |
|----------------|--------------------------------|--------------------------------|-----------------|---------|--------------------|----------------------|
| CE01           |                                | ContentEdge Monthly Commitment |                 |         | 100.000            | 75.000 7,500.00      |
| CEOC01         |                                | ContentEdge Usage Over Commit  |                 |         | 47.910             | 75.000 3,593.25      |
| STOR01         |                                | Data Storage Solution          |                 |         | 0.000              | 0.000 0.00           |
| STOROC01       |                                | Data Storage Solution Over     |                 |         | 0.000              | 0.000 0.00           |
| REP01          |                                | LUX Customer Reports           |                 |         | 1.000              | 250.000 250.00       |
| REP01          |                                | LUX Customer Reports           |                 |         | 1.000-             | 250.000 250.00-      |
| Comment:       |                                | Credit                         |                 |         |                    |                      |
| Invoice Total: |                                |                                |                 |         |                    | 11,093.25            |
| 0026592        | INV                            | 2/8/2007                       | A/R             | 0805014 | SetupAHost, Inc.   | 0207                 |
| Item Code      | Description                    |                                |                 |         | Quantity           | Unit Price Extension |
| CE01           | ContentEdge Monthly Commitment |                                |                 |         | 100.000            | 75.000 7,500.00      |
| CEOC01         | ContentEdge Usage Over Commit  |                                |                 |         | 36.840             | 75.000 2,763.00      |
| STOR01         | Data Storage Solution          |                                |                 |         | 0.000              | 0.000 0.00           |
| STOROC01       | Data Storage Solution Over     |                                |                 |         | 0.000              | 0.000 0.00           |
| REP01          | LUX Customer Reports           |                                |                 |         | 1.000              | 250.000 250.00       |
| REP01          | LUX Customer Reports           |                                |                 |         | 1.000-             | 250.000 250.00-      |
| Comment:       |                                | CREDIT                         |                 |         |                    |                      |
| Invoice Total: |                                |                                |                 |         |                    | 10,263.00            |
| 0027546        | INV                            | 3/9/2007                       | A/R             | 0805014 | SetupAHost, Inc.   | 0207                 |
| Item Code      | Description                    |                                |                 |         | Quantity           | Unit Price Extension |
| CE01           | ContentEdge Monthly Commitment |                                |                 |         | 100.000            | 75.000 7,500.00      |
| CEOC01         | ContentEdge Usage Over Commit  |                                |                 |         | 39.530             | 75.000 2,964.75      |
| STOR01         | Data Storage Solution          |                                |                 |         | 0.000              | 0.000 0.00           |
| STOROC01       | Data Storage Solution Over     |                                |                 |         | 0.000              | 0.000 0.00           |
| REP01          | LUX Customer Reports           |                                |                 |         | 1.000              | 250.000 250.00       |
| REP01          | LUX Customer Reports           |                                |                 |         | 1.000-             | 250.000 250.00-      |
| Comment:       |                                | CREDIT                         |                 |         |                    |                      |
| Invoice Total: |                                |                                |                 |         |                    | 10,464.75            |
| 0029542        | INV                            | 4/9/2007                       | A/R             | 0805014 | SetupAHost, Inc.   | 0207                 |
| Item Code      | Description                    |                                |                 |         | Quantity           | Unit Price Extension |
| CE01           | ContentEdge Monthly Commitment |                                |                 |         | 100.000            | 75.000 7,500.00      |
| CEOC01         | ContentEdge Usage Over Commit  |                                |                 |         | 28.460             | 75.000 2,134.50      |
| STOR01         | Data Storage Solution          |                                |                 |         | 0.000              | 0.000 0.00           |
| STOROC01       | Data Storage Solution Over     |                                |                 |         | 0.000              | 0.000 0.00           |
| REP01          | LUX Customer Reports           |                                |                 |         | 1.000              | 250.000 250.00       |
| REP01          | LUX Customer Reports           |                                |                 |         | 1.000-             | 250.000 250.00-      |
| Comment:       |                                | CREDIT                         |                 |         |                    |                      |
| Invoice Total: |                                |                                |                 |         |                    | 9,634.50             |
| 0031508        | INV                            | 5/9/2007                       | A/R             | 0805014 | SetupAHost, Inc.   | 0207                 |
| Item Code      | Description                    |                                |                 |         | Quantity           | Unit Price Extension |
| CE01           | ContentEdge Monthly Commitment |                                |                 |         | 100.000            | 75.000 7,500.00      |
| CEOC01         | ContentEdge Usage Over Commit  |                                |                 |         | 64.020             | 75.000 4,801.50      |
| STOR01         | Data Storage Solution          |                                |                 |         | 0.000              | 0.000 0.00           |
| STOROC01       | Data Storage Solution Over     |                                |                 |         | 0.000              | 0.000 0.00           |
| REP01          | LUX Customer Reports           |                                |                 |         | 1.000              | 250.000 250.00       |
| REP01          | LUX Customer Reports           |                                |                 |         | 1.000-             | 250.000 250.00-      |
| Comment:       |                                | CREDIT LUX REPORTS MONTHLY     |                 |         |                    |                      |
| Invoice Total: |                                |                                |                 |         |                    | 12,301.50            |
| 0033402        | INV                            | 6/12/2007                      | A/R             | 0805014 | SetupAHost, Inc.   | 0207                 |
| Item Code      | Description                    |                                |                 |         | Quantity           | Unit Price Extension |
| CE01           | ContentEdge Monthly Commitment |                                |                 |         | 100.000            | 75.000 7,500.00      |
| CEOC01         | ContentEdge Usage Over Commit  |                                |                 |         | 291.140            | 75.000 21,835.50     |
| STOR01         | Data Storage Solution          |                                |                 |         | 0.000              | 0.000 0.00           |
| STOROC01       | Data Storage Solution Over     |                                |                 |         | 0.000              | 0.000 0.00           |
| REP01          | LUX Customer Reports           |                                |                 |         | 1.000              | 250.000 250.00       |
| REP01          | LUX Customer Reports           |                                |                 |         | 1.000-             | 250.000 250.00-      |
| Comment:       |                                | CREDIT LUX REPORTS MONTHLY     |                 |         |                    |                      |
| Invoice Total: |                                |                                |                 |         |                    | 29,335.50            |
| 0034603        | INV                            | 7/12/2007                      | A/R             | 0805014 | SetupAHost, Inc.   | 0207                 |

Run Date: 11/13/2007 9:56:14AM

Page: 3

A/R Date: 11/13/2007

User Logon: James



Nov. 13. 2007 10:26AM

No. 0266 P. 1



Confidential

# ATTACHMENT A ORDER FORM

|                                                                                                                                                                                                                                                                                                                                                |          |                 |                  |                 |              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-----------------|------------------|-----------------|--------------|
| SetupAHost, Inc. ("Customer")                                                                                                                                                                                                                                                                                                                  |          |                 |                  | Issue Date:     | May 23, 2006 |
| SERVICES AND PRODUCTS                                                                                                                                                                                                                                                                                                                          |          |                 |                  | Number of Units | Unit Price   |
| LLNW ContentEdge CDN Solution (CNAME Setup - Upgrade)                                                                                                                                                                                                                                                                                          |          |                 |                  | 100             | \$7,500.00   |
| Limelight User Exchange (LUX) Reporting Package                                                                                                                                                                                                                                                                                                |          |                 |                  | 1               | \$250.00     |
| Limelight User Exchange (LUX) Reporting Package                                                                                                                                                                                                                                                                                                |          |                 |                  | 1               | (\$250.00)   |
| Professional Services-\$150/Hour (¼ hr. Minimum)                                                                                                                                                                                                                                                                                               |          |                 |                  |                 |              |
| Term:                                                                                                                                                                                                                                                                                                                                          | 12 Month | BURSTABLE RATE: | \$75.00 per Mbps | TOTALS:         | \$ 7,500.00  |
| NOTES:                                                                                                                                                                                                                                                                                                                                         |          |                 |                  |                 | \$0.00       |
| <ul style="list-style-type: none"> <li>Customer may commit to, in writing, and Limelight Networks will provide more bandwidth (Mbps/mo) at any time.</li> <li><b>The above pricing is valid till May 26<sup>th</sup>, 2005.</b></li> <li>Burstable bandwidth (anything over your committed level) is available at \$75.00 per/Mbps.</li> </ul> |          |                 |                  |                 |              |

## Company's Policy Regarding "95<sup>th</sup> Percentile" Bandwidth Utilization

On a monthly basis, Customer purchases a minimum amount of committed bandwidth for each Service for the full specified term. To account for the instances that Customer's traffic bursts over the minimum committed amount of bandwidth, the Company utilizes a billing method referred to as the "95<sup>th</sup> Percentile Rule" as defined below.

- Company shall invoice Customer on a monthly basis in advance for the minimum committed bandwidth at the rate set by this Order Form. The Company's SNMP bandwidth monitoring will sample (record a data point reflecting how much bandwidth Customer is utilizing at that particular instance) the inbound and outbound for each Service connection every 5 minutes and store those samples for a period of one month.
- At the end of the month, all the data samples for the inbound and outbound are collected and sorted from highest to lowest individually. The highest 5% of each the inbound and outbound are discarded, and the next highest remaining data sample on either the inbound or outbound is the "95<sup>th</sup> Percentile" number. This number is used as the basis for computation of any additional charges for that particular month of Service over the minimum committed bandwidth. If the 95<sup>th</sup> Percentile number falls below the monthly minimum committed amount, no additional charges will be assessed.

### Example:

Customer has committed to 20.0 Mbps per month. Company gathers all data samples for the month of Service and sorts them from highest to lowest discarding the top 5%. For purpose of example the 95<sup>th</sup> Percentile for the month of Service was 75 Mbps. Company will bill Customer for the additional charges of 75 Mbps less the previously invoiced 20 Mbps of contractually committed bandwidth, or 55 Mbps. The 55Mbps of "over usage" will be billed at the rate stated in this Order Form. Further, if the 95<sup>th</sup> Percentile calculation resulted in a number less than 20Mbps no additional charges would occur for that month.

The following is the formula based on a thirty (30)-day month:

$$\frac{1 \text{ Sample}}{5 \text{ Min}} * \frac{12}{1 \text{ Hour}} * \frac{24}{1 \text{ Day}} * \frac{30}{1 \text{ Month}} = 8,640 \text{ Maximum Total Samples/Month}$$

5% of 8640 Maximum Samples/Month = 432 Samples/Month discarded. The highest remaining data sample in the inbound or outbound would be the 95<sup>th</sup> Percentile.

|                                   |                                      |
|-----------------------------------|--------------------------------------|
| Limelight Networks, Inc.          | SetupAHost, Inc.                     |
| 2220 West 14 <sup>th</sup> Street | P.O Box 2122                         |
| Tempe, AZ 85281                   | Peterborough, Ontario K9J 7Y4 Canada |
| Michael Godlewski                 |                                      |
| Signature:                        | Signature:                           |
| Title: Vice President             | Title:                               |
| Date:                             | Date:                                |

Confidential

Page 1

LLNW0007

7/26/2005

Confidential Treatment  
Requested by Limelight  
Networks, Inc.

Attachment U

Page 336

Nov. 13. 2007 10:27AM

No. 0266 P. 2

| Order Type                                                                                                                                                                |                                                         | <input type="checkbox"/> TRIAL ORDER | <input type="checkbox"/> NEW ORDER    | <input checked="" type="checkbox"/> CHANGE ORDER |             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|--------------------------------------|---------------------------------------|--------------------------------------------------|-------------|
| <b>Sales Information</b>                                                                                                                                                  |                                                         |                                      |                                       |                                                  |             |
| Sales Rep Name                                                                                                                                                            | Mohit Nanubhai                                          | Sales Engineer Name                  | AJ                                    |                                                  |             |
| Sales Rep Email Address                                                                                                                                                   | mohit@lnw.com                                           | Sales Eng Email Address              | AJ@limelightnetworks.com              |                                                  |             |
| Customer Requested Due Date                                                                                                                                               | June 1st 2006                                           | Approval Date                        |                                       |                                                  |             |
| Contract Term                                                                                                                                                             | 12 Month                                                |                                      |                                       |                                                  |             |
| Reseller Name                                                                                                                                                             | none                                                    |                                      |                                       |                                                  |             |
| <b>Customer Information</b>                                                                                                                                               |                                                         |                                      | <b>Billing Information</b>            |                                                  |             |
| Company Name                                                                                                                                                              | SetupAHost, Inc                                         | Billing Name                         | SetupAHost, Inc                       |                                                  |             |
| Company Address                                                                                                                                                           | P O Box 2122                                            | Billing Address                      | P O Box 2122                          |                                                  |             |
| City, State, Zip                                                                                                                                                          | Peterborough, Ontario, K9J 7Y4 Canada                   | City, State, Zip                     | Peterborough, Ontario, K9J 7Y4 Canada |                                                  |             |
| Suite or Floor                                                                                                                                                            |                                                         | Suite or Floor                       |                                       |                                                  |             |
| Primary Contact Name                                                                                                                                                      | James Reno                                              | Billing Contact Name                 | James Reno                            |                                                  |             |
| Primary Contact Email                                                                                                                                                     | james@setupahost.net                                    | Billing Contact Email                | james@setupahost.net                  |                                                  |             |
| Primary Contact Phone                                                                                                                                                     | 513.685.0032 x 4501                                     | Billing Contact Phone                | 513.685.0032 x 4501                   |                                                  |             |
| Primary Contact FAX                                                                                                                                                       |                                                         | Billing Contact FAX                  |                                       |                                                  |             |
| Secondary Contact Name                                                                                                                                                    | James Reno                                              | Abuse Contact Name                   | James Reno                            |                                                  |             |
| Secondary Contact Email                                                                                                                                                   | james@setupahost.net                                    | Abuse Contact Email                  | james@setupahost.net                  |                                                  |             |
| Secondary Contact Phone                                                                                                                                                   | 513.685.0032 x 4501                                     | Abuse Contact Phone                  | 513.685.0032 x 4501                   |                                                  |             |
| Secondary Contact FAX                                                                                                                                                     |                                                         |                                      |                                       |                                                  |             |
| <b>ContentEdge</b>                                                                                                                                                        |                                                         |                                      |                                       |                                                  |             |
| <input type="checkbox"/> Limelight Origin <input checked="" type="checkbox"/> Customer Origin (CNAME)                                                                     |                                                         |                                      |                                       |                                                  |             |
| <b>MediaEdge On-Demand</b>                                                                                                                                                |                                                         |                                      |                                       |                                                  |             |
| <input type="checkbox"/> Windows Media <input type="checkbox"/> QUICKTIME <input type="checkbox"/> REAL <input type="checkbox"/> Flash (FCS)                              |                                                         |                                      |                                       |                                                  |             |
| <b>MediaEdge Live</b>                                                                                                                                                     |                                                         |                                      |                                       |                                                  |             |
| <input type="checkbox"/> Windows Media <input type="checkbox"/> QUICKTIME <input type="checkbox"/> REAL <input type="checkbox"/> MP3 Streaming                            |                                                         |                                      |                                       |                                                  |             |
| <b>Other Services</b>                                                                                                                                                     |                                                         |                                      |                                       |                                                  |             |
| <input type="checkbox"/> BulkGet <input type="checkbox"/> IPv4 <input type="checkbox"/> Colocation <input type="checkbox"/> RadioStream <input type="checkbox"/> Hardware |                                                         |                                      |                                       |                                                  |             |
| <b>ALL SERVICES BILLING INFORMATION</b>                                                                                                                                   |                                                         |                                      |                                       |                                                  |             |
| Billing Type                                                                                                                                                              | Description                                             | Price Per Unit                       | # of Units                            | One-Time                                         | MRR         |
| GB Transfer                                                                                                                                                               |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| GB Transfer Burst                                                                                                                                                         |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| Mbps 95/5                                                                                                                                                                 | Upgrading ContentEdge Solution from 15 mbps to 100 Mbps | \$ 75.00                             | 100                                   | \$ -                                             | \$ 7,500.00 |
| Mbps 95/5 Burst                                                                                                                                                           |                                                         | \$ 75.00                             |                                       | \$ -                                             | \$ -        |
| Mbps Peak                                                                                                                                                                 |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| Storage GB                                                                                                                                                                |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| Reports                                                                                                                                                                   |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| IPs                                                                                                                                                                       |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| Xconnect                                                                                                                                                                  |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| BulkGet                                                                                                                                                                   |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| RadioStream                                                                                                                                                               |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| MediaVault                                                                                                                                                                |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| Hardware                                                                                                                                                                  |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| Rack Space                                                                                                                                                                |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| Eng. Time                                                                                                                                                                 |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| Expedite Fee                                                                                                                                                              |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
| Other                                                                                                                                                                     |                                                         | \$ -                                 |                                       | \$ -                                             | \$ -        |
|                                                                                                                                                                           |                                                         |                                      | <b>Total</b>                          | \$ -                                             | \$ 7,500.00 |

905-248-3003

Nov. 13. 2007 10:27AM

No. 0266 P. 3

**Notes for SetupAHost,  
Inc**

Billing Change only: Customer is upgrading commitment from 15 mbps to 100 Mbps. This billing change needs to be active June 1st.

setuphost log.txt  
[cds264.sjc.llnw.net : 208.111.153.244]

58.9.15.223 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/bestsellerantivirus.com/Bestsell  
erAntivirus/install\_en.exe HTTP/1.0" 200 189851 "-" "-"  
/rlog34/squid/cds264.sjc.llnw.net/access.1193169601.0of1.log.70281.log.bz2 5714

74.170.214.86 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i704\_bot1  
.gif HTTP/1.0" 304 161  
"http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b500300  
01420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f0650  
03076c550a6a105e045f0547123d0c0c540703075f5107420355540f0616505c05010712025f0b08"  
"Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR  
1.1.4322; Media Center PC 4.0; Seekmo 10.0.341.0)"  
/rlog34/squid/cds264.sjc.llnw.net/access.1193169600.a400.70281.log.bz2 0

69.230.100.185 - - [23/Oct/2007:13:18:38 -0700] "HEAD  
http://content.onerateld.com.ref.cdn.setupahost.net/AntivirusSetupFree\_en.exe  
HTTP/1.0" 200 372 "-" "LocusSoftware, NetInstaller"  
/rlog34/squid/cds264.sjc.llnw.net/access.1193169600.a400.70281.log.bz2 310

74.170.214.86 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i704\_bot2  
.gif HTTP/1.0" 304 161  
"http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b500300  
01420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f0650  
03076c550a6a105e045f0547123d0c0c540703075f5107420355540f0616505c05010712025f0b08"  
"Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR  
1.1.4322; Media Center PC 4.0; Seekmo 10.0.341.0)"  
/rlog34/squid/cds264.sjc.llnw.net/access.1193169600.a400.70281.log.bz2 0

69.104.140.25 - - [23/Oct/2007:13:18:38 -0700] "HEAD  
http://content.onerateld.com.ref.cdn.setupahost.net/AntivirusSetupFree\_en.exe  
HTTP/1.0" 200 372 "-" "LocusSoftware, NetInstaller"  
/rlog34/squid/cds264.sjc.llnw.net/access.1193169600.a400.70281.log.bz2 307

76.221.203.53 - - [23/Oct/2007:13:18:38 -0700] "HEAD  
http://download.cdn.winsoftware.com.ref.cdn.setupahost.net/files/installers/winAntis  
pyware2007FreeInstall.exe HTTP/1.0" 200 368 "-" "Mozilla/4.0 (compatible; MSIE 6.0;  
windows NT 5.1; SV1; (R1 1.6))"  
/rlog34/squid/cds264.sjc.llnw.net/access.1193169600.a400.70281.log.bz2 306

69.33.52.108 - - [23/Oct/2007:13:18:38 -0700] "HEAD  
http://download.cdn.winsoftware.com.ref.cdn.setupahost.net/files/installers/winAntis  
pyware2007FreeInstall.exe HTTP/1.0" 200 368 "-" "Mozilla/4.0 (compatible; MSIE 6.0;  
windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
/rlog34/squid/cds264.sjc.llnw.net/access.1193169600.a400.70281.log.bz2 307

76.240.228.1 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/spyguardpro.com/SpyGuardPro/inst  
all\_en.exe HTTP/1.0" 200 189852 "-" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT  
5.1; FunWebProducts)"  
/rlog34/squid/cds264.sjc.llnw.net/access.1193169600.a400.70281.log.bz2 469

216.103.118.14 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i30\_image  
6.gif HTTP/1.0" 200 1356  
"http://bestsellerantivirus.com/data/index.php?51545b0b0d5d6c13093c091403394d126e5c5  
66654525d011e5f59085b43585e426a53593c04025c563c523c02570e586e5857666c56566c0c0903553  
900680a02020469025f6c420105045e5f0b6757090b000c6c065a0b5d090403500656080f04035200510  
2065205545b035e0d07535f5e5f556801025e0c57055e52555e0203065450520a5352550454080209055

Page 1

Attachment U

setuphost log.txt  
 558595852051f54545d085040570a0b0613555c5e01" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR 1.1.4322; Media Center PC 4.0; InfoPath.1; SpamBlockerUtility 4.8.4)"  
 /rlog34/squid/cds264.sjc.llnw.net/access.1193169600.a400.70281.log.bz2 0

24.195.224.174 - - [23/Oct/2007:08:03:32 -0700] "GET  
 http://content.onerated.com.ref.cdn.setupahost.net/static/www/data/img/en/i701\_line  
 2.jpg HTTP/1.0" 304 162  
 "http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b500300  
 01420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f0650  
 03056c550a6a105e045f0547123d0402530703075f5402420355540f0616505c05010212025f0b08"  
 "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.0.3705; .NET CLR  
 1.1.4322; Media Center PC 4.0; Seekmo 10.0.370.0)"  
 /rlog21/squid/cds264.sjc.llnw.net/access.1193151600.a400.70281.log.bz2 0

24.195.224.174 - - [23/Oct/2007:08:03:32 -0700] "GET  
 http://content.onerated.com.ref.cdn.setupahost.net/static/www/data/img/en/i701\_cor-  
 right-1.gif HTTP/1.0" 304 160  
 "http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b500300  
 01420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f0650  
 03056c550a6a105e045f0547123d0402530703075f5402420355540f0616505c05010212025f0b08"  
 "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.0.3705; .NET CLR  
 1.1.4322; Media Center PC 4.0; Seekmo 10.0.370.0)"  
 /rlog21/squid/cds264.sjc.llnw.net/access.1193151600.a400.70281.log.bz2 0

84.90.35.229 - - [23/Oct/2007:08:03:32 -0700] "GET  
 http://origin2.cdn.setupahost.net/sites/winantivirus.com/main/pages/scanner/img/ico3  
 .gif HTTP/1.0" 200 635  
 "http://winantivirus.com/download/2007/index.php?aid=swpwa7pdns\_pt\_pt\_ed2&lid=446&af  
 fid=pp\_2310370894&ax=0&p=&ex=1" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1;  
 sv1)" /rlog21/squid/cds264.sjc.llnw.net/access.1193151600.a400.70281.log.bz2 0

202.137.170.33 - - [23/Oct/2007:08:03:32 -0700] "GET  
 http://bsa.safetydownload.com.ref.cdn.setupahost.net/statice/paypages/landing/img/en  
 /i36\_bg-btn3.gif HTTP/1.0" 200 803  
 "http://storageprotector.com/clean/index.php?03500-80808-5f394-40d3a-47565-f0066-534  
 53-9030f-66535-50a40-53580-b040a-12431-66e00-5a390-65705-5b3a0-56602-04000-76f07-093  
 e6-6575e-67520-70257-66523-90553-06546-a075d-39150-70453-045f5-f6604-08545-15566-030  
 45-d050f-56060-d5400-03570-05051-05505-e055a-03030-10305-0d545-20000-075f6-90808-555  
 70-5015f-00550-f5050-550d0-4075f-0b060-7045c-50570-b0a06-03510-50c53-175d0-30b05-445  
 c1-25b04-50171-25f5b-03" "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1;  
 InfoPath.1; Ninemsn Optimised; AU; Ninemsn Optimised; AU)"  
 /rlog21/squid/cds264.sjc.llnw.net/access.1193151600.a400.70281.log.bz2 0

75.61.126.6 - - [23/Oct/2007:08:03:32 -0700] "HEAD  
 http://download.cdn.winsoftware.com.ref.cdn.setupahost.net/files/installers/winAntis  
 pyware2007FreeInstall.exe HTTP/1.0" 200 368 "-" "Mozilla/4.0 (compatible; MSIE 6.0;  
 Windows NT 5.1; FunWebProducts; YPC 3.2.0; .NET CLR 1.1.4322)"  
 /rlog21/squid/cds264.sjc.llnw.net/access.1193151600.a400.70281.log.bz2 306

84.90.35.229 - - [23/Oct/2007:08:03:32 -0700] "GET  
 http://origin2.cdn.setupahost.net/sites/winantivirus.com/main/pages/scanner/img/ico4  
 .gif HTTP/1.0" 200 626  
 "http://winantivirus.com/download/2007/index.php?aid=swpwa7pdns\_pt\_pt\_ed2&lid=446&af  
 fid=pp\_2310370894&ax=0&p=&ex=1" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1;  
 sv1)" /rlog21/squid/cds264.sjc.llnw.net/access.1193151600.a400.70281.log.bz2 0

222.127.226.229 - - [23/Oct/2007:08:03:32 -0700] "GET  
 http://content.onerated.com.ref.cdn.setupahost.net/static/www/data/img/en/i28a\_bg1.  
 gif HTTP/1.0" 304 160  
 "http://avsystemcare.com/data/?gai=swdark&gli=6253\_ao\_4078\_0\_1888\_ao\_&cmpname=null&4  
 5080108&mt\_info=4078\_0\_1888" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1;  
 sv1)" /rlog21/squid/cds264.sjc.llnw.net/access.1193151600.a400.70281.log.bz2 0

Page 2

Attachment U

## setuphost log.txt

222.127.226.229 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i28a\_icon  
2.gif HTTP/1.0" 304 160  
"http://avsystemcare.com/data/?gai=swdark&gli=6253\_ao\_4078\_0\_1888\_ao\_&cmpname=null&4  
5080108&mt\_info=4078\_0\_1888" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1;  
SV1)" /rlog21/squid/cds264.sjc.llnw.net/access.1193151600.a400.70281.log.bz2 0

[cds497.sjc.llnw.net : 208.111.148.137]

70.66.224.217 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/pcprivacytool.com/PCPrivacyTo  
ol/installer\_en.exe HTTP/1.0" 200 131082  
"http://pcprivacytool.com/privacy/index.php?590c170b451411390107066953566c015d695d55  
4707130d59470d0255010c6f590a3a0207505239563c5405070f6c055c691e5053440811406a07035107  
0e0001505d1053115c574013580e06115b140e0708" "Mozilla/4.0 (compatible; MSIE 7.0;  
windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506)"  
/rlog90/squid/cds497.sjc.llnw.net/access.1193169600.0of1.log.17586.log.bz2 5315

68.63.215.121 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/img\_6  
01/znak.gif HTTP/1.0" 200 2684  
"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a43436c505  
6675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e6  
8056f075754506d535e6d455404450f111569090502080f08090008155317040613400b5353521458410  
f52" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

68.63.215.121 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/img\_6  
01/xrest0.gif HTTP/1.0" 200 1473  
"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a43436c505  
6675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e6  
8056f075754506d535e6d455404450f111569090502080f08090008155317040613400b5353521458410  
f52" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

201.19.154.56 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/img\_6  
02/fon.gif HTTP/1.0" 200 440  
"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a54426c454  
c675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e6  
8056f075754516d535e6d455404450f111569090406080f0809000d155317040613400b5353511458410  
f52" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8  
01/icon\_09.gif HTTP/1.0" 200 1344  
"http://winanonymos.com/privacy/?air=gsfcronwan&lir=5599\_ao\_4404\_0\_4135\_ao\_ao\_4404  
\_0\_4095\_ao\_ao\_4404\_0\_4135\_ao\_ao\_4500\_0\_4640\_ao\_&afr=gs\_3602970951&ar=&er=&edr=&hp=  
&cmpname=null&160a085205&mt\_info=4500\_0\_4640" "Mozilla/4.0 (compatible; MSIE 6.0;  
windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET

Page 3

Attachment U

setuphost log.txt  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p801/icon\_07.gif HTTP/1.0" 200 1434  
"http://winanonymouse.com/privacy/?air=gsfcronwan&lir=5599\_ao\_4404\_0\_4135\_ao\_ao\_4404\_0\_4095\_ao\_ao\_4404\_0\_4135\_ao\_ao\_4500\_0\_4640\_ao\_&afr=gs\_3602970951&ar=&er=&edr=&hp=&cmpname=null&l60a085205&mt\_info=4500\_0\_4640" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

72.254.2.151 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i44\_boton.gif HTTP/1.0" 200 4844  
"http://bestsellerantivirus.com/data/index.php?51545b0b04435507043c100c5f394d126e5c566654525d011e5f59085b05010d0e6a53593c040757563c523c02570e586e5857666c56566c0c0903553900680a02020369025f6c420105045e56156753010d000d050e0e02091e520d030d061e510806024557595957" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; FunWebProducts-MyWay)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

68.199.181.253 - - [23/Oct/2007:13:18:38 -0700] "HEAD  
http://download.cdn.winsoftware.com.ref.cdn.setupahost.net/files/installers/winAntispyware2007FreeInstall.exe HTTP/1.0" 200 368 "-" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 309

201.19.154.56 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/img\_602/fon\_top.gif HTTP/1.0" 200 634  
"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a54426c454c675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e68056f075754516d535e6d455404450f111569090406080f0809000d155317040613400b5353511458410f52" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

12.215.123.194 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/download2/u\_top\_left.gif HTTP/1.0" 200 579  
"http://bestsellerantivirus.com/data/install2.php?51545b0b0d5d6c13093c0f064507670a4608674c40685c5d675f5005546f52405f41144406435a1e035e5345560a515c5f5c4f4a6c56566c0c090d513900680b07030b69025f6c3b070c3d5700500c3e01660a0d040766525767130600560a565b6a040e5108063b565b202575530e5107787a0d02067d707a01015920060f0a0e007474257675223950202672540e25740c0f7b70030b020e7901235408010f00770a705608015c5445055e0555" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; Seekmo 10.0.275.0)" /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

12.215.123.194 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/download2/lines.gif HTTP/1.0" 200 421  
"http://bestsellerantivirus.com/data/install2.php?51545b0b0d5d6c13093c0f064507670a4608674c40685c5d675f5005546f52405f41144406435a1e035e5345560a515c5f5c4f4a6c56566c0c090d513900680b07030b69025f6c3b070c3d5700500c3e01660a0d040766525767130600560a565b6a040e5108063b565b202575530e5107787a0d02067d707a01015920060f0a0e007474257675223950202672540e25740c0f7b70030b020e7901235408010f00770a705608015c5445055e0555" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; Seekmo 10.0.275.0)" /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

69.110.177.181 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/spacer.gif HTTP/1.0" 200 400  
"http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b5003001420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f06503026c550a6a105e045f0547123d0d02570503075f5100420355540f0616500b0f00" "Mozilla/4.0

Page 4

Attachment U

setuphost log.txt  
 (compatible; MSIE 6.0; windows NT 5.1; SV1)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

72.254.2.151 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i44\_ug3.g  
 if HTTP/1.0" 200 465  
 "http://bestsellerantivirus.com/data/index.php?51545b0b04435507043c100c5f394d126e5c5  
 66654525d011e5f59085b05010d0e6a53593c040757563c523c02570e586e5857666c56566c0c0903553  
 900680a02020369025f6c420105045e56156753010d000d050e0e02091e520d030d061e5108060245575  
 95957" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1;  
 FunWebProducts-Myway)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

71.131.25.217 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i44\_ic3.g  
 if HTTP/1.0" 304 160  
 "http://antispyswaresuite.com/data/index.php?02005c5f5e1052010008473d4c4b39040c6f045c  
 5c0b12535a0c0d5750000e170207535f5e106b51515304500e085f54531604555d04051251580456435e  
 5d0c54" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

69.110.177.181 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/pcsecures  
 ystem.com/logo.gif HTTP/1.0" 200 5936  
 "http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b500300  
 01420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f0650  
 03026c550a6a105e045f0547123d0d02570503075f5100420355540f0616500b0f00" "Mozilla/4.0  
 (compatible; MSIE 6.0; windows NT 5.1; SV1)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

69.110.177.181 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/man.gif  
 HTTP/1.0" 200 11908  
 "http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b500300  
 01420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f0650  
 03026c550a6a105e045f0547123d0d02570503075f5100420355540f0616500b0f00" "Mozilla/4.0  
 (compatible; MSIE 6.0; windows NT 5.1; SV1)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.214.130.84 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i30\_image  
 5.gif HTTP/1.0" 200 1167  
 "http://avsystemcare.com/data/index.php?52545a0d56094d540c5214106a5a424a06b17456d51  
 583e515d530245010e0d085a4016520d0a0042560b5904" "Mozilla/4.0 (compatible; MSIE 6.0;  
 windows NT 5.1; .NET CLR 1.1.4322)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticcd/www/landing/img/en/p8  
 01/icon\_11.gif HTTP/1.0" 200 1574  
 "http://winanonymous.com/privacy/?air=gsfcronwan&lir=5599\_ao\_4404\_0\_4135\_ao\_ao\_4404  
 \_0\_4095\_ao\_ao\_4404\_0\_4135\_ao\_ao\_4500\_0\_4640\_ao\_&afr=gs\_3602970951&ar=&er=&edr=&hp=  
 &cmpname=null&160a085205&mt\_info=4500\_0\_4640" "Mozilla/4.0 (compatible; MSIE 6.0;  
 windows NT 5.1; SV1)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

69.110.177.181 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/avsc\_bann  
 er.gif HTTP/1.0" 200 14766  
 "http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b500300  
 01420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f0650  
 03026c550a6a105e045f0547123d0d02570503075f5100420355540f0616500b0f00" "Mozilla/4.0  
 (compatible; MSIE 6.0; windows NT 5.1; SV1)"

Page 5

Attachment U

```

 setuphost log.txt
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8
01/icon_16.gif HTTP/1.0" 200 1379
"http://winanonymous.com/privacy/?air=gsfcronwan&lir=5599_ao_4404_0_4135_ao_ao_4404
_0_4095_ao_ao_4404_0_4135_ao_ao_4500_0_4640_ao_&afr=gs_3602970951&ar=&er=&edr=&hp=
&cmpname=null&160a085205&mt_info=4500_0_4640" "Mozilla/4.0 (compatible; MSIE 6.0;
windows NT 5.1; SV1)"
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

189.142.222.14 - - [23/Oct/2007:13:18:38 -0700] "GET
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/es/he
ader_bg.gif HTTP/1.0" 200 617
"http://driveproteccion.com/pcsegura/?air=gsfcronwan&lir=5598_ao_4500_2463_198_ao_a
o_3669_800_1401_ao_&afr=gs_3536570951&ar=&er=&edr=&hp=&cmpname=null&tmn=c11&mt_info=
4500_2463_198&tmn=null" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1)"
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

83.58.178.236 - - [23/Oct/2007:13:18:38 -0700] "GET
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/es/i55_top3.
gif HTTP/1.0" 200 7423
"http://exterminadorvirus.com/alarma/index.php?0343530405450554066a460e0b3b5c463b5
0413a5c5c510117084f03590705005a6a53563d025704546a043e56550f0c3b545d3a66595f6c05550f5
63b030400556a010f55073c560b6a12070312580803466d560c01000206540057551456545f041449030
b560242525e5c54" "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; InfoPath.1;
.NET CLR 2.0.50727; .NET CLR 1.1.4322)"
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 309

83.58.178.236 - - [23/Oct/2007:13:18:38 -0700] "GET
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/es/i55_lupa.
gif HTTP/1.0" 200 9489
"http://exterminadorvirus.com/alarma/index.php?0343530405450554066a460e0b3b5c463b5
0413a5c5c510117084f03590705005a6a53563d025704546a043e56550f0c3b545d3a66595f6c05550f5
63b030400556a010f55073c560b6a12070312580803466d560c01000206540057551456545f041449030
b560242525e5c54" "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; InfoPath.1;
.NET CLR 2.0.50727; .NET CLR 1.1.4322)"
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 307

68.63.215.121 - - [23/Oct/2007:13:18:38 -0700] "GET
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/img_6
01/footer.gif HTTP/1.0" 200 588
"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a43436c505
6675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e6
8056f075754506d535e6d455404450f111569090502080f08090008155317040613400b5353521458410
f52" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR 1.1.4322)"
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8
01/icon_17.gif HTTP/1.0" 200 1270
"http://winanonymous.com/privacy/?air=gsfcronwan&lir=5599_ao_4404_0_4135_ao_ao_4404
_0_4095_ao_ao_4404_0_4135_ao_ao_4500_0_4640_ao_&afr=gs_3602970951&ar=&er=&edr=&hp=
&cmpname=null&160a085205&mt_info=4500_0_4640" "Mozilla/4.0 (compatible; MSIE 6.0;
windows NT 5.1; SV1)"
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8
01/icon_18.gif HTTP/1.0" 200 1362
"http://winanonymous.com/privacy/?air=gsfcronwan&lir=5599_ao_4404_0_4135_ao_ao_4404
_0_4095_ao_ao_4404_0_4135_ao_ao_4500_0_4640_ao_&afr=gs_3602970951&ar=&er=&edr=&hp=
&cmpname=null&160a085205&mt_info=4500_0_4640" "Mozilla/4.0 (compatible; MSIE 6.0;

```

Page 6

Attachment U

setuphost log.txt

windows NT 5.1; SV1)"

/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

12.215.123.194 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/download2  
/note.gif HTTP/1.0" 200 3835

"http://bestsellerantivirus.com/data/install12.php?51545b0b0d5d6c13093c0f064507670a46  
08674c40685c5d675f5005546f52405f41144406435ale035e5345560a515c5f5c4f4a6c56566c0c090d  
513900680b07030b69025f6c3b070c3d5700500c3e01660a0d040766525767130600560a565b6a040e51  
08063b565b202575530e5107787a0d02067d707a01015920060f0a0e007474257675223950202672540e  
25740c0f7b70030b020e7901235408010f00770a705608015c5445055e0555" "Mozilla/4.0  
(compatible; MSIE 6.0; windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; seekmo  
10.0.275.0)" /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2  
0

68.63.215.121 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/img\_6  
01/top\_line.jpg HTTP/1.0" 200 2588

"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a43436c505  
6675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e6  
8056f075754506d535e6d455404450f111569090502080f08090008155317040613400b5353521458410  
f52" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

66.146.177.122 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/i3  
0\_im\_04.gif HTTP/1.0" 200 4268

"http://trasheraser.com/privacy/index.php?0250470e01170502560752416846476b485e6d035d  
145316090b17083b52096d5708040a3d556a0550575b6c565c6b12420b01561f0c110d54"  
"Mozilla/4.0 (compatible; MSIE 7.0; windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET  
CLR 3.0.04506)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 312

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8  
01/bottom\_23.gif HTTP/1.0" 200 4653

"http://winanonymouse.com/privacy/?air=gsfcronwan&lir=5599\_ao\_4404\_0\_4135\_ao\_ao\_4404  
\_0\_4095\_ao\_ao\_4404\_0\_4135\_ao\_ao\_4500\_0\_4640\_ao\_&afr=gs\_3602970951&ar=&er=&edr=&hp=  
&cmpname=null&l60a085205&mt\_info=4500\_0\_4640" "Mozilla/4.0 (compatible; MSIE 6.0;  
windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

71.131.25.217 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i44\_ic2.g  
if HTTP/1.0" 304 160

"http://antispwarsuite.com/data/index.php?02005c5f5e1052010008473d4c4b39040c6f045c  
5c0b12535a0c0d5750000e170207535f5e106b51515304500e085f54531604555d04051251580456435e  
5d0c54" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8  
01/fon\_07.jpg HTTP/1.0" 200 881

"http://winanonymouse.com/privacy/?air=gsfcronwan&lir=5599\_ao\_4404\_0\_4135\_ao\_ao\_4404  
\_0\_4095\_ao\_ao\_4404\_0\_4135\_ao\_ao\_4500\_0\_4640\_ao\_&afr=gs\_3602970951&ar=&er=&edr=&hp=  
&cmpname=null&l60a085205&mt\_info=4500\_0\_4640" "Mozilla/4.0 (compatible; MSIE 6.0;  
windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

24.218.77.156 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://bsa.safetydownload.com.ref.cdn.setupahost.net/statice/paypages/landing/img/en  
/i607\_main.gif HTTP/1.0" 200 18005

"http://systemerrorfixer.com/clean/index.php?57520-d0d0b-54681-1566a-51165-f4500-671  
Page 7

Attachment U

setuphost log.txt

41-06c57-0d390-65457-13520-f0b05-045d5-d500f-6f045-66852-080d0-53b04-6d020-e5856-6c5  
30-c393c-510a6-a0352-540d3-9016d-01510-95566-56096-66a55-0b6b0-60000-503c0-36d57-535  
30-83a54-583c3-d5909-6e060-05c09-3a096-8570c-03053-b555d-6e1e0-40255-0f0d0-b3c06-5d0  
70-f563d-5e070-90007-50565-30e03-000d0-40500-570b0-75d54-05050-a515e-56560-75351-050  
46-70207-0a040-05457-01555-60f00-00000-60409-0b555-60a51-5b5e5-20601-06515-1525d-405  
45-70e55-16004-90a50-09021-2175e-0f00" "Mozilla/4.0 (compatible; MSIE 6.0; Windows  
NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR 1.1.4322; Media Center PC 4.0; Seekmo  
10.0.341.0)" /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2  
0

24.218.77.156 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://bsa.safetydownload.com.ref.cdn.setupahost.net/static/paypages/landing/img/en  
/i607\_button.gif HTTP/1.0" 200 4457  
"http://systemerrorfixer.com/clean/index.php?57520-d0d0b-54681-1566a-51165-f4500-671  
41-06c57-0d390-65457-13520-f0b05-045d5-d500f-6f045-66852-080d0-53b04-6d020-e5856-6c5  
30-c393c-510a6-a0352-540d3-9016d-01510-95566-56096-66a55-0b6b0-60000-503c0-36d57-535  
30-83a54-583c3-d5909-6e060-05c09-3a096-8570c-03053-b555d-6e1e0-40255-0f0d0-b3c06-5d0  
70-f563d-5e070-90007-50565-30e03-000d0-40500-570b0-75d54-05050-a515e-56560-75351-050  
46-70207-0a040-05457-01555-60f00-00000-60409-0b555-60a51-5b5e5-20601-06515-1525d-405  
45-70e55-16004-90a50-09021-2175e-0f00" "Mozilla/4.0 (compatible; MSIE 6.0; windows  
NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR 1.1.4322; Media Center PC 4.0; Seekmo  
10.0.341.0)" /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2  
0

71.131.25.217 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i44\_ug1.g  
if HTTP/1.0" 304 159  
"http://antispysware suite.com/data/index.php?02005c5f5e1052010008473d4c4b39040c6f045c  
5c0b12535a0c0d5750000e170207535f5e106b51515304500e085f54531604555d04051251580456435e  
5d0c54" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; sv1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

122.161.137.217 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/i2  
6\_part7.gif HTTP/1.0" 304 160  
"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a5f5e6c505  
6675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c545767515a6600015d0e6  
8056f075754566d535e6d455404450f1115690406030f0f0809000a155317040613400b57554558420c0  
3" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8  
01/fon\_center\_con\_03.jpg HTTP/1.0" 200 785  
"http://winanonymouse.com/privacy/?air=gsfcronwan&lir=5599\_ao\_4404\_0\_4135\_ao\_\_ao\_4404  
\_0\_4095\_ao\_\_ao\_4404\_0\_4135\_ao\_\_ao\_4500\_0\_4640\_ao\_\_&afr=gs\_3602970951&ar=&er=&edr=&hp=  
&cmpname=null&l60a085205&mt\_info=4500\_0\_4640" "Mozilla/4.0 (compatible; MSIE 6.0;  
windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8  
01/logo\_03.jpg HTTP/1.0" 200 41555  
"http://winanonymouse.com/privacy/?air=gsfcronwan&lir=5599\_ao\_4404\_0\_4135\_ao\_\_ao\_4404  
\_0\_4095\_ao\_\_ao\_4404\_0\_4135\_ao\_\_ao\_4500\_0\_4640\_ao\_\_&afr=gs\_3602970951&ar=&er=&edr=&hp=  
&cmpname=null&l60a085205&mt\_info=4500\_0\_4640" "Mozilla/4.0 (compatible; MSIE 6.0;  
windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

122.161.137.217 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/i2  
6\_bg1.gif HTTP/1.0" 304 159  
"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a5f5e6c505

Page 8

Attachment U

setuphost log.txt  
6675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e6  
8056f075754566d535e6d455404450f1115690406030f0f0809000a155317040613400b57554558420c0  
3" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

81.203.251.90 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateid.com.ref.cdn.setupahost.net/static/www/data/img/es/i52\_space  
r.gif HTTP/1.0" 200 387  
"http://defensaantimalware.com/alarma/index.php?0743530558100d58061716096c0651056950  
466955443c5050050010581457090d504b515b3a595e3a575109023e036b020602036f560c6a6b055d69  
00510306390703080d3a0c035d5b3e585c3e15515708041040565e0006" "Mozilla/4.0  
(compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 1.1.4322)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 307

71.131.25.217 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://content.onerateid.com.ref.cdn.setupahost.net/static/www/data/img/en/i44\_boton  
.gif HTTP/1.0" 304 161  
"http://antispysuite.com/data/index.php?02005c5f5e1052010008473d4c4b39040c6f045c  
5c0b12535a0c0d5750000e170207535f5e106b51515304500e085f54531604555d04051251580456435e  
5d0c54" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

201.19.154.56 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/img\_6  
02/fon\_znak.jpg HTTP/1.0" 200 3661  
"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a54426c454  
c675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e6  
8056f075754516d535e6d455404450f111569090406080f0809000d155317040613400b5353511458410  
f52" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

68.63.215.121 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/img\_6  
01/bgbot.gif HTTP/1.0" 200 1327  
"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a43436c505  
6675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e6  
8056f075754506d535e6d455404450f111569090502080f08090008155317040613400b5353521458410  
f52" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

66.146.177.122 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/i3  
0\_landing-cara-diablo.gif HTTP/1.0" 200 8476  
"http://trasheraser.com/privacy/index.php?0250470e01170502560752416846476b485e6d035d  
145316090b17083b52096d5708040a3d556a0550575b6c565c6b12420b01561f0c110d54"  
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET  
CLR 3.0.04506)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 316

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8  
01/fon\_cont\_03.gif HTTP/1.0" 200 859  
"http://winanonymouse.com/privacy/?air=gsfcronwan&lir=5599\_ao\_4404\_0\_4135\_ao\_ao\_4404  
\_0\_4095\_ao\_ao\_4404\_0\_4135\_ao\_ao\_4500\_0\_4640\_ao\_&afr=gs\_3602970951&ar=&er=&edr=&hp=  
&cmname=null&160a085205&mt\_info=4500\_0\_4640" "Mozilla/4.0 (compatible; MSIE 6.0;  
Windows NT 5.1; SV1)"  
/rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8  
01/fon\_cont\_06.gif HTTP/1.0" 200 1050  
"http://winanonymouse.com/privacy/?air=gsfcronwan&lir=5599\_ao\_4404\_0\_4135\_ao\_ao\_4404  
\_0\_4095\_ao\_ao\_4404\_0\_4135\_ao\_ao\_4500\_0\_4640\_ao\_&afr=gs\_3602970951&ar=&er=&edr=&hp=

Page 9

setuphost log.txt  
 &cmpname=null&160a085205&mt\_info=4500\_0\_4640" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

82.46.9.216 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/i26\_part3.gif HTTP/1.0" 304 161  
 "http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a435b6c4554675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e68056f025553526d535e6d455404450f11156903020c0f0d0f000c0d0610004b0a0416465851551458410f52" "Mozilla/5.0 (Windows; U; Windows NT 5.1; pl; rv:1.8.1.8) Gecko/20071008 Firefox/2.0.0.8"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

76.193.217.16 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p801/footer\_03.jpg HTTP/1.0" 200 22046  
 "http://winanonymouse.com/privacy/?air=gsfcronwan&lir=5599\_ao\_4404\_0\_4135\_ao\_ao\_4404\_0\_4095\_ao\_ao\_4404\_0\_4135\_ao\_ao\_4500\_0\_4640\_ao\_&afr=gs\_3602970951&ar=&er=&edr=&hp=&cmpname=null&160a085205&mt\_info=4500\_0\_4640" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

84.197.98.199 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p52/bah\_top\_01.gif HTTP/1.0" 200 2254  
 "http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a45556c5b54675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e68056f025553526d535e6d455404450f1115690904010d0f0809000b155317040613400b50514558420c03" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

71.131.25.217 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i44\_ug2.gif HTTP/1.0" 304 161  
 "http://antispyswaresuite.com/data/index.php?02005c5f5e1052010008473d4c4b39040c6f045c5c0b12535a0c0d5750000e170207535f5e106b51515304500e085f54531604555d04051251580456435e5d0c54" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

81.203.251.90 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/es/i52\_vrt.gif HTTP/1.0" 200 449  
 "http://defensaantimalware.com/alarma/index.php?0743530558100d58061716096c0651056950466955443c5050050010581457090d504b515b3a595e3a575109023e036b020602036f560c6a6b055d6900510306390703080d3a0c035d5b3e585c3e15515708041040565e0006" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 1.1.4322)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 307

71.131.25.217 - - [23/Oct/2007:13:18:38 -0700] "GET  
 http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i44\_f3.gif HTTP/1.0" 304 161  
 "http://antispyswaresuite.com/data/index.php?02005c5f5e1052010008473d4c4b39040c6f045c5c0b12535a0c0d5750000e170207535f5e106b51515304500e085f54531604555d04051251580456435e5d0c54" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

86.136.156.8 - - [23/Oct/2007:08:03:32 -0700] "GET  
 http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p52/top\_03.gif HTTP/1.0" 200 872  
 "http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a435b6c5056675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e68056f025553526d535e6d455404450f11156902040d000c0f000d000210004b0a0416465856511458410f52" "Mozilla/5.0 (Windows; U; Windows NT 5.1; pl; rv:1.8.1.8) Gecko/20071008 Firefox/2.0.0.8"  
 /rlog82/squid/cds497.sjc.llnw.net/access.1193169600.a400.17586.log.bz2 0

Page 10

Attachment U

setuphost log.txt

f52" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.1)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

84.193.192.157 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i704\_vt.gif HTTP/1.0" 200 7148  
"http://winsecureav.com/data/index.php?52030b0b5444525068125b0f07103b565d695f0967545451014051590f0e53540c5b445155510954443a0a5957515c03080e08541e545d500e5710525b0456551305080b02" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" /rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

125.62.113.85 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i29a\_btn1.gif HTTP/1.0" 200 999  
"http://bestsellerantivirus.com/data/index.php?51545b0b04435507043c100c5f39510f6e5c56654525d011e5f59085b05010d0e6a53593c040757563c523c02570e586e5857666c56566c0c0903553900680a02020a69025f6c420105045e561567550808010e030e09021e5f59045b01115f0b070b10045a0e55" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

210.194.85.213 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://bsa.safetydownload.com.ref.cdn.setupahost.net/static/paypages/landing/img/jp/i7\_img\_4.gif HTTP/1.0" 200 6542  
"http://hadodoraibugado.com/soshi/index.php?5c070-85911-42595-b6d5e-57390-b0568-0e043-e0f56-6b0b0-33d08-043e5-f533c-5a556-90c00-3b085-66b58-536b5-c073e-0e563-b0f00-3a5d5-53e08-033d0-f006a-58026-f5e46-54470-e0e5e-09595-74d5f-083e0-5583b-51505-4046b-513d5-05254-546a5-30c6f-125c0-25c53-44445-e0f03" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 308

80.171.126.51 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticcd/www/landing/img/en/p52/bottom\_03.gif HTTP/1.0" 304 160  
"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a52556c515d675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e68056f025553526d535e6d455404450f111569010b01000c0f000d000210004b0a0416465856511458410f52" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; FunWebProducts)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 1

84.57.130.92 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://bsa.safetydownload.com.ref.cdn.setupahost.net/static/paypages/landing/img/de/i36\_Scan.swf HTTP/1.0" 200 18502  
"http://diskretter.com/kontroller/index.php?59020-d5f11-03015-55f0b-01466-a0001-6b540-36f58-500a1-5580f-5e0e5-25441-595c6-d020b-3d520-20401-6" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

84.57.130.92 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://bsa.safetydownload.com.ref.cdn.setupahost.net/static/paypages/landing/img/de/i36\_t1.gif HTTP/1.0" 200 1851  
"http://diskretter.com/kontroller/index.php?59020-d5f11-03015-55f0b-01466-a0001-6b540-36f58-500a1-5580f-5e0e5-25441-595c6-d020b-3d520-20401-6c526-b0005-55516-b5109-6f155-f480e-00551-14053-0c09" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

84.193.192.157 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i704\_win\_logo.gif HTTP/1.0" 200 834  
"http://winsecureav.com/data/index.php?52030b0b5444525068125b0f07103b565d695f0967545451014051590f0e53540c5b445155510954443a0a5957515c03080e08541e545d500e5710525b0456551305080b02" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" /rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

Page 11

## setuphost log.txt

71.141.96.77 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/im  
g\_815/bg.gif HTTP/1.0" 200 1635  
"http://gubbishremover.com/privacy/index.php?5059420a475e09535850555c6c10106b535e3d0  
7574b0217540a4509500f400e6e515f68070557076f096d070753526b575f3d44430408000d455d44045  
0" "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 6.0; SLCC1; .NET CLR 2.0.50727;  
.NET CLR 3.0.04506)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 318

71.141.96.77 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/im  
g\_815/man.gif HTTP/1.0" 200 21972  
"http://gubbishremover.com/privacy/index.php?5059420a475e09535850555c6c10106b535e3d0  
7574b0217540a4509500f400e6e515f68070557076f096d070753526b575f3d44430408000d455d44045  
0" "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 6.0; SLCC1; .NET CLR 2.0.50727;  
.NET CLR 3.0.04506)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 331

211.213.27.90 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/cont\_top\_  
bg.gif HTTP/1.0" 200 749  
"http://trustedprotection.com/data/index.php?53595d0e041752543e17143a52413d0a0c67520  
351031f025e5d0d540d0d0c13535e520e04176b0359545d52090a5250455f590308001f020f0200521e5  
35e0805" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

71.97.146.55 - - [23/Oct/2007:08:03:32 -0700] "HEAD  
http://download.cdn.winsoftware.com.ref.cdn.setupahost.net/files/installers/winAntis  
pyware2007FreeInstall.exe HTTP/1.0" 200 368 "-" "Mozilla/4.0 (compatible; MSIE 6.0;  
windows NT 5.1)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 306

125.162.94.37 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8  
02/center2.gif HTTP/1.0" 200 417  
"http://pcprivacytool.com/privacy/?cmpname=swpgdc&air=swp\_gdc\_net&lir=747\_ao\_4133\_0\_  
2692\_ao\_&afr=pp\_99770908&&cmpname=null&48585d0604&mit\_info=4133\_0\_2692" "Mozilla/4.0  
(compatible; MSIE 7.0; windows NT 5.1; .NET CLR 2.0.50727)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

69.69.39.2 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i701\_bg2.  
gif HTTP/1.0" 200 510  
"http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b500300  
01420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f0650  
03056c550a6a105e045f0547123d0407550003075f5402420355540f0616505c05010212025f0b08"  
"Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; iebar; HbTools 4.7.0)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 3

69.69.39.2 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i701\_line  
3.gif HTTP/1.0" 200 677  
"http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b500300  
01420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f0650  
03056c550a6a105e045f0547123d0407550003075f5402420355540f0616505c05010212025f0b08"  
"Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; iebar; HbTools 4.7.0)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

125.162.94.37 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p8  
02/top.gif HTTP/1.0" 200 643  
"http://pcprivacytool.com/privacy/?cmpname=swpgdc&air=swp\_gdc\_net&lir=747\_ao\_4133\_0\_

Page 12

setuphost log.txt

2692\_ao\_&afr=pp\_99770908&&cmpname=null&48585d0604&mt\_info=4133\_0\_2692" "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; .NET CLR 2.0.50727)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

125.62.113.85 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i29a\_btn2.gif HTTP/1.0" 200 1141  
"http://bestsellerantivirus.com/data/index.php?51545b0b04435507043c100c5f39510f6e5c56654525d011e5f59085b05010d0e6a53593c040757563c523c02570e586e5857666c56566c0c0903553900680a02020a69025f6c420105045e561567550808010e030e09021e5f59045b01115f0b070b10045a0e55" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

84.193.192.157 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i704\_str.gif HTTP/1.0" 200 475  
"http://winsecureav.com/data/index.php?52030b0b5444525068125b0f07103b565d695f0967545451014051590f0e53540c5b445155510954443a0a5957515c03080e08541e545d500e5710525b0456551305080b02" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR 1.1.4322)" /rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

211.213.27.90 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/black\_corners/b-topleft.gif HTTP/1.0" 200 518  
"http://trustedprotection.com/data/index.php?53595d0e041752543e17143a52413d0a0c67520351031f025e5d0d540d0d0c13535e520e04176b0359545d52090a5250455f590308001f020f0200521e535e0805" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

69.69.39.2 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i701\_line2.jpg HTTP/1.0" 200 1429  
"http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b50030001420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f065003056c550a6a105e045f0547123d0407550003075f5402420355540f0616505c05010212025f0b08" "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; iebar; HbTools 4.7.0)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

71.141.96.77 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticcd/www/landing/img/en/img\_815/main.jpg HTTP/1.0" 200 13355  
"http://gubbishremover.com/privacy/index.php?5059420a475e09535850555c6c10106b535e3d07574b0217540a4509500f400e6e515f68070557076f096d070753526b575f3d44430408000d455d440450" "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 318

69.69.39.2 - - [23/Oct/2007:08:03:32 -0700] "GET  
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i701\_cor-right-1.gif HTTP/1.0" 200 885  
"http://pcsecuresystem.com/data/index.php?56525d5846414b035459413d17466b035a6b50030001420355580f02090e526d505c6b56020f0a3d0967065651006b075b6b68070b6c575301046d076f065003056c550a6a105e045f0547123d0407550003075f5402420355540f0616505c05010212025f0b08" "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; iebar; HbTools 4.7.0)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

69.33.52.108 - - [23/Oct/2007:08:03:32 -0700] "HEAD  
http://download.cdn.winsoftware.com.ref.cdn.setupahost.net/files/installers/winAntispyware2007FreeInstall.exe HTTP/1.0" 200 368 "-" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR 1.1.4322)"  
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 306

84.57.130.92 - - [23/Oct/2007:08:03:32 -0700] "GET

```

 setuphost log.txt
http://bsa.safetydownload.com.ref.cdn.setupahost.net/static/paypages/landing/img/de
/i36_icon2.gif HTTP/1.0" 200 1854
"http://diskretter.com/kontroller/index.php?59020-d5f11-03015-55f0b-01466-a0001-6b54
0-36f58-500a1-5580f-5e0e5-25441-595c6-d020b-3d520-20401-6c526-b0005-55516-b5109-6f15
5-f480e-00551-14053-0c09" "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1)"
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

71.141.96.77 - - [23/Oct/2007:08:03:32 -0700] "GET
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/im
g_815/circle.gif HTTP/1.0" 200 449
"http://gubbishremover.com/privacy/index.php?5059420a475e09535850555c6c10106b535e3d0
7574b0217540a4509500f400e6e515f68070557076f096d070753526b575f3d44430408000d455d44045
0" "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 6.0; SLCC1; .NET CLR 2.0.50727;
.NET CLR 3.0.04506)"
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 316

86.136.156.8 - - [23/Oct/2007:08:03:32 -0700] "GET
http://sec.storageguardsoft.com.ref.cdn.setupahost.net/staticd/www/landing/img/en/p5
2/warning_03.gif HTTP/1.0" 200 798
"http://yourprivacyguard.com/privacy/index.php?040a110f41464002583d5056023a435b6c505
6675d54470b155a0c4b0a00090f563c025d6d02055a023d076d505701066c54576767515a6600015d0e6
8056f025553526d535e6d455404450f11156902040d000c0f000d000210004b0a0416465856511458410
f52" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR 1.1.4322;
.NET CLR 2.0.50727; InfoPath.1)"
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

84.193.192.157 - - [23/Oct/2007:08:03:32 -0700] "GET
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i704_spac
er.gif HTTP/1.0" 200 399
"http://winsecureav.com/data/index.php?52030b0b5444525068125b0f07103b565d695f0967545
451014051590f0e53540c5b445155510954443a0a5957515c03080e08541e545d500e5710525b0456551
305080b02" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET CLR
1.1.4322)" /rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

125.62.113.85 - - [23/Oct/2007:08:03:32 -0700] "GET
http://content.onerateld.com.ref.cdn.setupahost.net/static/www/data/img/en/i29a_btn3
.gif HTTP/1.0" 200 785
"http://bestsellerantivirus.com/data/index.php?51545b0b04435507043c100c5f39510f6e5c5
66654525d011e5f59085b05010d0e6a53593c040757563c523c02570e586e5857666c56566c0c0903553
900680a02020a69025f6c420105045e561567550808010e030e09021e5f59045b01115f0b070b10045a0
e55" "Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1)"
/rlog34/squid/cds497.sjc.llnw.net/access.1193151600.a400.17586.log.bz2 0

86.10.111.121 - - [23/Oct/2007:08:03:32 -0700] "GET
http://content.onerateld.com.ref.cdn.setupahost.net/winspycontrol.com/winspyControl/
install_en.exe HTTP/1.0" 200 189851 "-" "Mozilla/4.0 (compatible; MSIE 6.0; windows
NT 5.1; .NET CLR 1.1.4322)"
/rlog65/squid/cds497.sjc.llnw.net/access.1193151601.0of1.long.17586.log.bz2 6105

```


3:19:47 PM 3/20/2008


http:

ErrorProtector

## ErrorProtector

100% SATISFACTION GUARANTEE ON ALL ORDERS

 **Your Purchase is Backed  
By Our 30-Day Money  
Back Guarantee!**

 **Fully Secure &  
Encrypted Ordering -  
Even Safer Than Over  
the Phone.**

### Your Payment Information

**Payment Type** Credit Card

**Card Number**

**Expiration Date** 03 2008

**CVV2 Number**

### Your Name And Address

**Name**

**Email ID**

**Address**

**City**

**Country** United States

**Telephone**

**Password** ☐ Generate ☐ Let me enter

**Certificate**

General Details Certification Path


Show: <All>

| Field               | Value                             |
|---------------------|-----------------------------------|
| Version             | V3                                |
| Serial number       | 7d 9d 2b 50 ed fa 03 cf ab 61 ... |
| Signature algorithm | sha1RSA                           |
| Issuer              | UTN-USERFirst-Hardware, htt...    |
| Valid from          | Thursday, October 18, 2007 7...   |
| Valid to            | Saturday, November 01, 2008...    |
| Subject             | pay.errorprotector.com, Com...    |
| Public key          | RSA (1024 Bits)                   |

CN = pay.errorprotector.com  
OU = Comodo InstantSSL  
OU = Hosted by Setup A Host, Inc  
OU = WebSecurity Dep.  
O = Errorprotector Inc  
STREET = 2635 Willow St  
L = Pasadena  
S = CA  
PostalCode = 90804

Copy to File...

OK

  
[Extended Download Service](#)

Done

start 10:10:10.20 - VMWare 9 Internet Explorer 100% 3:19 PM

2:22:13 PM 3/20/2008

https://secure.drivecleaner.com/payment/?ad=keyin&amp;link=keyin&amp;product=452&amp;aff=

DriveCleaner

## DriveCleaner

100% SATISFACTION GUARANTEE ON ALL ORDERS



Your Purchase is Backed  
By Our 30-Day Money  
Back Guarantee!



Fully Secure &  
Encrypted Ordering  
Even Safer Than Over  
the Phone.

### Your Payment Information

Payment Type Credit Card

Card Number

Expiration Date

CVV2 Number

[What is CVV?](#)

### Your Name and Address

Name

Email ID

Address

City

Country

United States

Telephone

Password

[Generate](#)

**Certificate**

General Details Certification Path

Show: <All>

| Field               | Value                            |
|---------------------|----------------------------------|
| Version             | V3                               |
| Serial number       | 6d 37 41 1d 0c 47 de 08 a8...    |
| Signature algorithm | sha1RSA                          |
| Issuer              | UTN-USERFirst-Hardware, htt...   |
| Valid from          | Thursday, January 03, 2008 7...  |
| Valid to            | Friday, January 09, 2009 6:59... |
| Subject             | secure.drivecleaner.com, Com...  |
| Public key          | RSA (1024 Bits)                  |

CN = secure.drivecleaner.com  
OU = Comodo InstantSSL  
OU = Hosted by Setup A Host, Inc  
OU = WebSecurity Dep.  
O = DriveCleaner Inc  
STREET = 32 Maxwell Road #03-07  
L = Singapore  
S = N/A  
PostalCode = 069115

[Copy to File...](#)

[OK](#)

[Extended Download Service](#)

Done

Internet

100%

2:22 PM

https://secure.fantazybill.com/payment/?sku\_name=MC\_EN\_B\_00&aid=mcbill&affid=421\_93487\_1\_en\_00

MalwareCrush - Payment Page

## MalwareCrush

### Your Payment Information

Payment Type: Credit Card  
 Card Number:   
 Expiration Date:    
 CVV2 Number:  [What is CVV?](#)

### Your Name and Address

Name:   
 Email ID:   
 Address:   
 City:   
 Country: Afghanistan  
 Telephone:   
 Password:  ☐ Generate ☐ Let me enter

*Items in **bold** are required. Information is needed for credit card verification even for download orders. It is never shared with other companies.*

**SECURE PURCHASE**

SecurePay

TrustChoice

Terms  
You are  
This is a

**CRUSH**

How to use  
the software

**Certificate**

General Details Certification Path

Show: <All>

| Field               | Value                                   |
|---------------------|-----------------------------------------|
| Version             | V3                                      |
| Serial number       | 00 f3 71 ce 27 a4 e4 1c 24 e4 ...       |
| Signature algorithm | sha1RSA                                 |
| Issuer              | UTN-USERFirst-Hardware, htt...          |
| Valid from          | Sunday, May 13, 2007 7:00:0...          |
| Valid to            | Tuesday, May 13, 2008 6:59:...          |
| <b>Issued to</b>    | <b>secure.fantazybill.com, Comod...</b> |
| Public key          | RSA (1024 Bits)                         |

CN = secure.fantazybill.com  
 OU = Comodo InstantSSL  
 OU = Hosted by Setup A Host, Inc  
 OU = WebSecurity Dep.  
 O = Fantazybill Inc.  
 STREET = 115 E. Railroad  
 L = Green River  
 S = WY  
 PostalCode = 82935

[Copy to File...](#)

**OK**

Done Internet 100% 3:29 PM

start 10.10.10.20 - www 9 Internet Explorer Auto-Protect Results

8:45:22 AM 3/21/2008

https://sale.pcsecuresystem.com/payment/?qpid=742&amp;gsid=207&amp;gai=keyin&amp;gli=keyin

PCSecureSystem - Payment Page

## PCSecureSystem

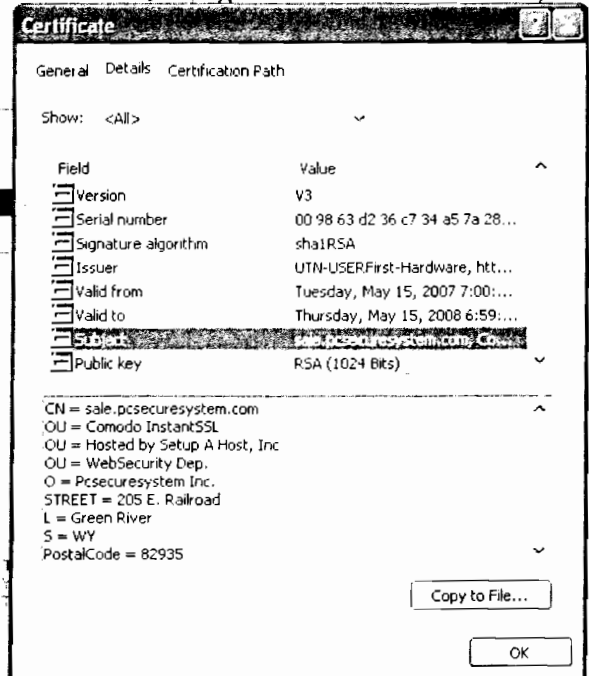
### Your Payment Information

Payment Type Credit Card  
Card Number  
Expiration Date  
CVV2 Number [What is CVV?](#)

### Your Name and Address

Name  
Email ID  
Address  
City  
Country United States  
Telephone  
Password  
☐ Generate  
☐ Let me enter

Items in **bold** are required. Information is needed for credit card verification even for download orders. It is never shared with other companies.

**SECURE PURCHASE**

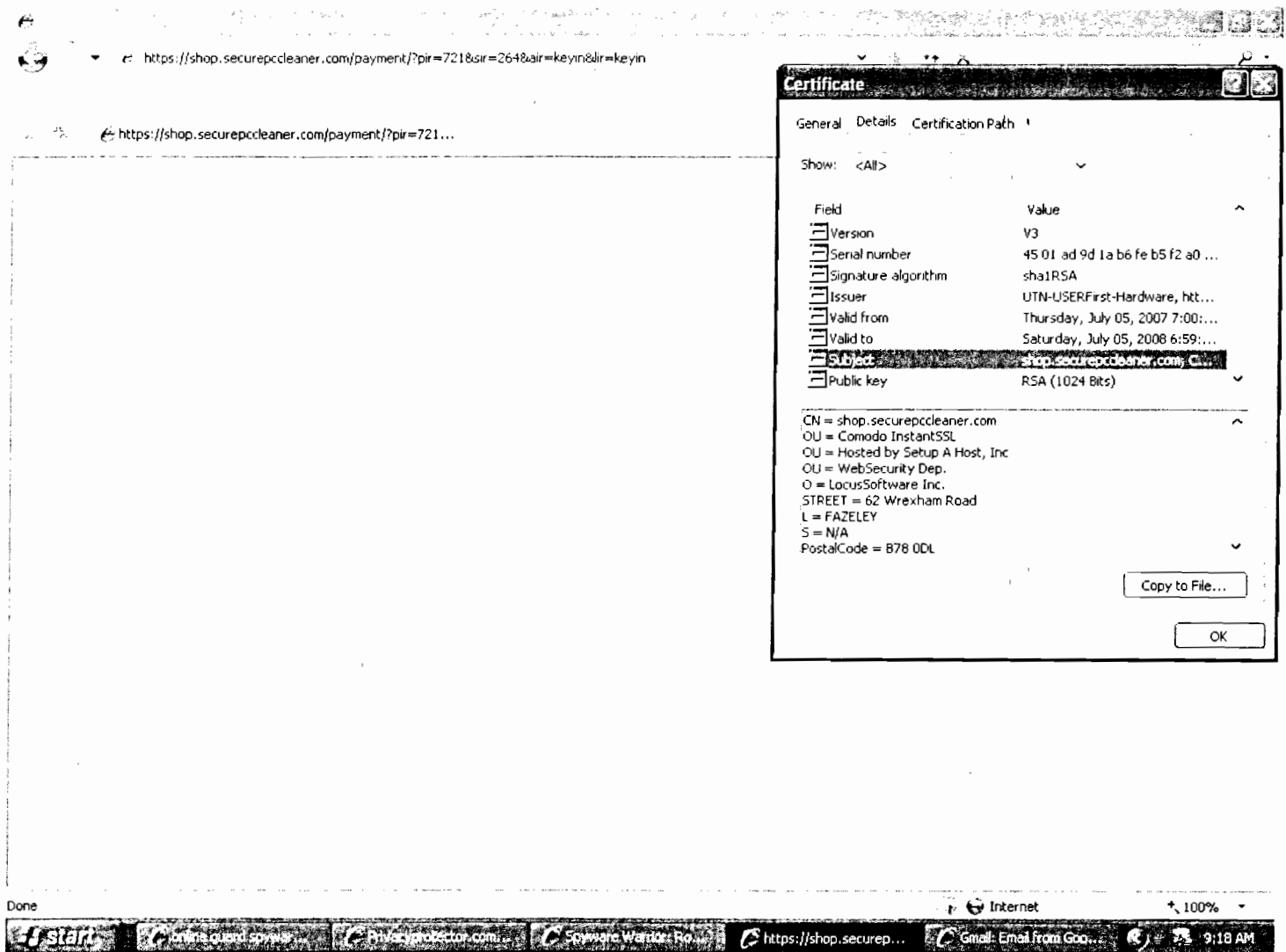
Done

Internet

100%



9:18:37 AM 3/21/2008





|            |              |                                                              |        |       |         |      |      |
|------------|--------------|--------------------------------------------------------------|--------|-------|---------|------|------|
| DATE:      | DOCUMENT ID  | DESCRIPTION                                                  | FILING | EXPED | PENALTY | CERT | COPY |
| 12/12/2005 | 200534303068 | AGENT ADDRESS<br>CHANGE/LIMITED/LIABILITY/PARTNER<br>S (LAD) | 25.00  | 00    | 00      | 00   | 00   |

**Receipt**

This is not a bill. Please do not remit payment.

BYTEHOSTING INTERNET SERVICES  
1833 E OHIO PIKE  
STE 104  
AMELIA, OH 45102-2086

# STATE OF OHIO CERTIFICATE

**Ohio Secretary of State, J. Kenneth Blackwell**

1361215

It is hereby certified that the Secretary of State of Ohio has custody of the business records for

**BYTEHOSTING INTERNET SERVICES, LLC**

and, that said business records show the filing and recording of:

Document(s)

**AGENT ADDRESS CHANGE/LIMITED/LIABILITY/PARTNERS**

Document No(s):

**200534303068**

United States of America  
State of Ohio  
Office of the Secretary of State

Witness my hand and the seal of  
the Secretary of State at Columbus.  
Ohio this 5th day of December,  
A.D. 2005.

  
Ohio Secretary of State

Attachment W

Prescribed by **J. Kenneth Blackwell**

Ohio Secretary of State

Central Ohio: (614) 466-3910

Toll Free: 1-877-SOS-FILE (1-877-767-3453)

www.state.oh.us/sos

e-mail: busserv@sos.state.oh.us

Expedite this Form: (Select One)

Mail Expedite one of the Following:

☐ Yes

PO Box 1390

Columbus, OH 43216

\*\*\* Requires an additional fee of \$100 \*\*\*

☒ No

PO Box 788

Columbus, OH 43216

**STATUTORY AGENT UPDATE**

(For Domestic or Foreign, Profit or Non-Profit)

Filing Fee \$25.00

THE UNDERSIGNED DESIRING TO FILE A:

**(CHECK ONLY ONE (1) BOX)**

(1) Subsequent Appointment of Agent

☐ Corp ☐ LP (165-AGS)☐ LLC (171-LSA)

(2) Change of Address of an Agent

☐ Corp ☐ LP (145-AGA)☒ LLC (144-LAD)

(3) Resignation of Agent

☐ Corp ☐ LP (155-AGR)☐ LLC (153-LAG)Complete ALL of the general information in this section for the box checked above.

Name of Entity

Byte Hosting Internet Services, LLC

Charter or  
Registration No.

1361215

Name of Current Agent

James M. Reno

Complete the information in this section if box (1) is checked.

Name and Address of  
New Agent

(Name)

(Street)

NOTE: P.O. Box Addresses are NOT acceptable.

Ohio

(City)

(County)

(State)

(Zip Code)

**ACCEPTANCE OF APPOINTMENT**

The Undersigned, \_\_\_\_\_, named herein as

the Statutory agent for, \_\_\_\_\_, hereby acknowledges and  
accepts the appointment of statutory agent for said entity.

Signature: \_\_\_\_\_

(Statutory Agent)

\* If the entity listed is a foreign corporation, the agent does not have to sign the Acceptance of Appointment

Complete the information in this section if box (2) is checked.

Old Address of Agent

1833 E Ohio Pike STE 104  
(Street) NOTE: P.O. Box Addresses are NOT acceptable.Amelia  
(City)Ohio  
(State)45102  
(Zip Code)

New Address of Agent

3864 McMann Road STE A  
(Street) NOTE: P.O. Box Addresses are NOT acceptable.Cincinnati  
(City)Ohio  
(State)45245  
(Zip Code)

Complete the information in this section if box (3) is checked.

Is this agent resigning?

☐ Yes☐ NoCurrent or last known address  
of the entity's principal office  
where a copy of this Resignation  
of Agent was sent as of the date  
of filing or prior to the date filed

(Street)


NOTE: P.O. Box Addresses are NOT acceptable.

(City)

(State)

(Zip Code)

## REQUIRED

Must be authenticated (signed) by an  
authorized representative  
(See Instructions)  
Authorized Representative11/16/05  
Date



|            |              |                                           |        |        |         |      |      |
|------------|--------------|-------------------------------------------|--------|--------|---------|------|------|
| DATE:      | DOCUMENT ID  | DESCRIPTION                               | FILING | EXPED  | PENALTY | CERT | COPY |
| 06/12/2007 | 200716202138 | ARTICLES OF ORGANIZATION/DOM<br>LLC (LCA) | 125.00 | 100.00 | 00      | 00   | 5.00 |

**Receipt**

This is not a bill. Please do not remit payment.

SMALLBIZ.COM  
PO BOX 13092  
TUCSON, AZ 85732

# STATE OF OHIO CERTIFICATE

Ohio Secretary of State, Jennifer Brunner

1706012

It is hereby certified that the Secretary of State of Ohio has custody of the business records for

**BYTECENTER WEB SERVICES, LLC**

and, that said business records show the filing and recording of:

Document(s)

**ARTICLES OF ORGANIZATION/DOM. LLC**

Document No(s):

**200716202138**

United States of America  
State of Ohio  
Office of the Secretary of State

Witness my hand and the seal of  
the Secretary of State at Columbus,  
Ohio this 11th day of June, A.D.  
2007.

Ohio Secretary of State



## Prescribed by:

Ohio Secretary of State  
Central Ohio: (614) 466-3910  
Toll Free: 1-877-SOS-FILE (1-877-767-3453)

www.state.oh.us/sos  
e-mail: busserv@sos.state.oh.us

## Expedite this Form: (Select One)

## Mail Form to one of the Following:

- ☒ Yes PO Box 1390  
Columbus, OH 43216  
-- Requires an additional fee of \$100 --
- ☐ No PO Box 670  
Columbus, OH 43216

### ORGANIZATION / REGISTRATION OF LIMITED LIABILITY COMPANY

(Domestic or Foreign)

Filing Fee \$125.00

THE UNDERSIGNED DESIRING TO FILE A:

## (CHECK ONLY ONE (1) BOX)

|                                                                                                                                           |                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <p>(1) <input checked="" type="checkbox"/> Articles of Organization for Domestic Limited Liability Company<br/>(115-LCA)<br/>ORC 1705</p> | <p>(2) <input type="checkbox"/> Application for Registration of Foreign Limited Liability Company<br/>(106-LFA)<br/>ORC 1705</p> |
| (Date of Formation)                                                                                                                       | (State)                                                                                                                          |

## Complete the general information in this section for the box checked above.

Name ByteCenter Web Services, LLC

☐ Check here if additional provisions are attached

\* If box (1) is checked, name must include one of the following endings: limited liability company, limited, Ltd, L.t.d., LLC, L.L.C.

## Complete the information in this section if box (1) is checked.

Effective Date (Optional) \_\_\_\_\_ Date specified can be no more than 90 days after date of filing. If a date is specified, the date must be a date on or after the date of filing.  
(mm/dd/yyyy)

This limited liability company shall exist for \_\_\_\_\_ (Period of existence)  
(Optional)

Purpose Provide internet-based services to public  
(Optional)

The address to which interested persons may direct requests for copies of any operating agreement and any bylaws of this limited liability company is \_\_\_\_\_

(Optional)

\_\_\_\_\_  
(Name)

\_\_\_\_\_  
(Street) NOTE: P.O. Box Addresses are NOT acceptable.

\_\_\_\_\_  
(City) \_\_\_\_\_ (State) \_\_\_\_\_ (Zip Code)

Complete the information in this section if box (1) is checked Cont.

### ORIGINAL APPOINTMENT OF AGENT

The undersigned authorized member, manager or representative of  
ByteCenter Web Services, LLC  
(name of limited liability company)

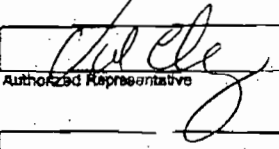
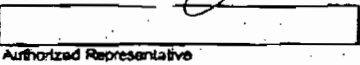
hereby appoint the following to be statutory agent upon whom any process, notice or demand required or permitted by statute to be served upon the limited liability company may be served. The name and address of the agent is:

James M. Reno  
(Name of Agent)

3864 McMann Road STE. A  
(Street) NOTE: P.O. Box Addresses are NOT acceptable.

Cincinnati Ohio 45245  
(City) (State) (Zip Code)

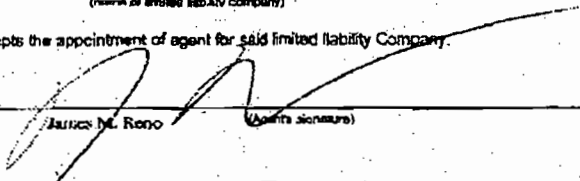
Must be authenticated by an authorized representative

|                                                                                   |                   |
|-----------------------------------------------------------------------------------|-------------------|
|  | <u>05/24/2007</u> |
| Authorized Representative                                                         | Date              |
|  |                   |
| Authorized Representative                                                         | Date              |

### ACCEPTANCE OF APPOINTMENT

The undersigned, named herein as the statutory agent for  
ByteCenter Web Services, LLC  
(name of limited liability company)

hereby acknowledges and accepts the appointment of agent for said limited liability company.

James M. Reno   
(Agent's signature)

PLEASE SIGN PAGE (3) AND SUBMIT COMPLETED DOCUMENT

200716982138  
 Complete the information in this section if box (2) is checked.

The address to which interested persons may direct requests for copies of any operating agreement and any bylaws of this limited liability company is

(Name)

(Street)

NOTE: P.O. Box Addresses are NOT acceptable.

(City)

(State)

(Zip Code)

The name under which the foreign limited liability company desires to transact business in Ohio is

The limited liability company hereby appoints the following as its agent upon whom process against the limited liability company may be served in the state of Ohio. The name and complete address of the agent is

(Name)

(Street)

NOTE: P.O. Box Addresses are NOT acceptable.

(City)

Ohio

(State)

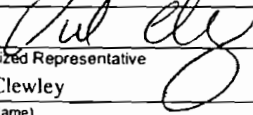
(Zip Code)

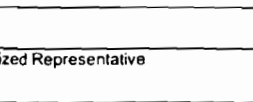
The limited liability company irrevocably consents to service of process on the agent listed above as long as the authority of the agent continues, and to service of process upon the OHIO SECRETARY OF STATE if:

- the agent cannot be found, or
- the limited liability company fails to designate another agent when required to do so, or
- the limited liability company's registration to do business in Ohio expires or is cancelled.

#### REQUIRED

Must be authenticated (signed)  
 by an authorized representative  
 (See Instructions)

  
 Authorized Representative Date  
 Val Clewley Organizer  
 (Print Name)

  
 Authorized Representative Date  
 (Print Name)

